الجمهورية الجزائرية الديمقراطية الشعبية

The People's Democratic Republic of Algeria

العالي و البحث العلمي وزارة التعليم

Ministry of Higher Education and Scientific Research

جامعة عمار ثليجي – الأغواط

University Amar Telidji of Laghouat

Faculty : Technology

Departement : Electronics

Domain: Science and Technology (ST)

Field: Telecommunications

Speciality: Telecommunications networks

Course Handout (Practical Work)

Intended for students of: Master's Level: 1st Year

IP ROUTING

Presented by: Mohammed Yousri Silaa

MCA, University of Laghouat

Email : Moh.silaa@lagh-univ.dz

Academic year : 2025/2026

Contents

General Introduction

The internet can be understood as a vast coalition of interconnected autonomous networks, each operating under its own set of policies, services, costs, and administrative domains. These independent networks collectively ensure the seamless exchange of data across the globe, enabling communication between millions of devices and users [1]. At the core of this structure lies the concept of the local area network (LAN), which can be defined as a group of devices that share a common communication medium, either wired or wireless, to facilitate the transmission and exchange of information among different entities within a limited geographical area [2].

LANs play a foundational role in modern communication systems, as they represent the building blocks upon which larger and more complex internetworks are established. Depending on their design, LANs can connect to other networks through routers and switches, forming regional, national, or even international infrastructures. The efficiency of these networks depends largely on the standards and protocols that govern how information is transmitted, routed, and delivered to its destination. These standards can be classified according to multiple criteria, such as their organizational architecture, physical distance, data transmission speed, and the type of information being exchanged [3].

Within the context of computer networking education, the study of LANs, switching, and routing is particularly crucial. Students of network engineering and telecommunications must not only acquire theoretical knowledge but also develop practical skills to configure and troubleshoot real networking equipment. This is why laboratory sessions and simulation tools have become essential components of modern curricula. One widely used tool is Cisco Packet Tracer, a simulation environment that allows learners to create, configure, and test virtual networks in a safe and controlled setting [4].

The present work has been developed as part of practical sessions in IP routing for Master's students in networks and telecommunications (R&T). Its primary aim is to provide learners with a structured environment to deepen their understanding of fundamental networking concepts, while also offering hands-on exposure to the configuration of network devices such as switches and routers. More specifically, the focus is on enabling students to:

1. Become familiar with basic network equipment and their operating principles.

2. Analyze the behavior of different routing strategies, such as static and dynamic routing.

3. Gain practical experience in troubleshooting and optimizing local and inter-network con-

nections.

Ultimately, this document serves as a pedagogical guide for students and beginners who wish to acquire foundational knowledge of switching and IP routing using Cisco Packet Tracer. It is structured into seven chapters, each addressing specific concepts and practices necessary for building a comprehensive understanding of modern networking. By combining theoretical foundations with practical applications, this work contributes to bridging the gap between abstract concepts and their implementation in real-world scenarios, thereby equipping students with the skills required to navigate the challenges of today's interconnected digital world.

This document also serves as a practical guide for learners who wish to gain fundamental knowledge of switching and IP routing through the use of the Cisco Packet Tracer simulation tool. The material is structured into seven chapters for clarity and progression.

Course Technical Information:

- **Course Title:** IP Routing (PW)
- **Credits:** 2
- **Coefficient:** 1
- **Semester Hours (15 weeks):** 22h 30min
- **Assessment Method:** Continuous Assessment 100%

The practical works (PWs) included in this course are designed to provide hands-on experience with key networking concepts. They guide students step by step through the configuration of switches, VLANs, routing protocols, redundant links, and EtherChannel, allowing learners to apply theoretical knowledge in simulated or real network environments. These exercises progressively build the skills needed to design, implement, and manage modern IP networks effectively.

- **PW1:** Basic configuration of a switch (CISCO platform). Simulation using Packet Tracer or practical work on real platforms.
- **PW2:** Creation and configuration of a VLAN-segmented network.
- **PW3:** Configuration of inter-VLAN routing. Simulation using Packet Tracer or practical work on real platforms.
- **PW4:** Creation of a network with redundant links. Simulation using Packet Tracer or practical work on real platforms.

- **PW5:** Configuration of the EtherChannel protocol between switches. Simulation using Packet Tracer or practical work on real platforms.
- **PW6:** Implementation of static routing. Simulation using Packet Tracer or practical work on real platforms.
- **PW7:** Implementation of dynamic routing (RIPv2, EIGRP, and OSPF). Simulation using Packet Tracer or practical work on real platforms.

By the end of this set of practical sessions, students will be able to simulate and troubleshoot a variety of configuration issues on Cisco networking devices. This experience will help them develop a clearer and more straightforward understanding of how different networking systems operate and interact.

I hope this document helps readers gain a clearer understanding of the topics discussed and serves as a useful reference for their studies or research. Feedback, constructive comments, and suggestions for improvement are appreciated, as they help enhance the quality of the work.

PW1: Basic configuration of a switch (CISCO platform). Simulation using Packet Tracer or practical work on real platforms.

I Learning objective

In this practical work, the focus is on understanding the fundamental role of a Cisco switch and on applying the essential configuration commands. The main objectives are:

- Practice simulating a small network using Cisco Packet Tracer and making the necessary settings on the devices used.
- Practice making the necessary settings for the switch using a console cable or remotely via Telnet using the simulation program Cisco Packet Tracer.
- Practice how to connect devices and the type of cables used.
- Gain a clear understanding of the basic function of a switch.
- Erase any existing configuration from the switch.
- Check and analyze the default settings of the switch.
- Build and apply a basic configuration for the switch.
- Testing the connection.

II Theoretical background

II.1 Network basics

A local area network (LAN) is a group of devices connected to share information and resources over wired or wireless links. Data on a LAN is transmitted as packets, and switches play a key role in forwarding them based on media access control (MAC) addresses. Networks can vary by size, speed, topology, and type of data transmitted [5].

Cisco switches

Cisco switches operate mainly at Layer 2 and can be configured both locally and remotely:

a) Local access or console port: Through the console port using a serial connection. This port that connects the switch to either an asynchronous terminal or a personal computer running a terminal emulation program such as Microsoft HyperTerminal (MHT), using a serial cable (usually short in length). The default configuration parameters are listed in Table .1 [**?**, **?**]:

Table .1: Console port parameters and description

Parameter / Feature	**Description**
Console port	A serial interface that connects the switch to an asynchronous terminal or a PC running a terminal emulation program (e.g., Microsoft HyperTerminal) using a short serial cable.
Speed (Baud rate)	9600 bps (default transmission speed).
Data bits	8 bits per data frame.
Start bit	1 bit to indicate the beginning of a data frame.
Stop bit	1 bit to indicate the end of a data frame.
Parity	None (no error checking).
Flow control	None (no flow control mechanism used).
Importance	Essential for initial switch configuration, especially when no internet protocol (IP) protocol is configured, preventing remote access.

b) Remote access: Once an IP address is configured on a switch, it can be accessed and managed remotely through its network interfaces. Common methods for remote configuration include:

- **Virtual terminals (Virtual teletype (VTY)):** Accessing the switch via asynchronous terminal emulation software, such as a Telnet client.
- **Trivial file transfer protocol (TFTP) servers:** Facilitating the transfer of configuration files to and from the switch.
- **Network management stations:** Using simple network management protocol (SNMP) based management platforms, for example, CiscoWorks or HP OpenView, to monitor and configure the device.

Switch configuration modes

Cisco switches support multiple configuration modes, each providing different levels of access and control. Understanding these modes is essential for effective switch management and network configuration.

a) User EXEC mode (Switch>)

The User EXEC mode is the default mode when a user first accesses a switch via console or remote connection. It allows basic monitoring commands, such as viewing interface status, checking basic statistics, and verifying connectivity using commands like packet internet or inter-network groper (ping) or show interfaces. However, configuration changes cannot be made in this mode. This mode is useful for users who need to check the status of the switch without the risk of altering its configuration.

b) Privileged EXEC mode (Switch#)

The privileged EXEC mode is accessed by entering the enable command from the User EXEC mode. It provides full access to configuration commands and advanced troubleshooting features. In this mode, administrators can view detailed system information, save or restore configurations, monitor network performance, and perform diagnostic tests. Commands such as show running-config, show version, and reload are executed in this mode. To exit this mode, the user can type exit, end, or press CTRL+Z.

c) Global configuration mode (Switch(config)#)

The global configuration mode is entered from the privileged EXEC mode using the configure terminal command. This mode allows administrators to make changes that affect the entire switch. Common tasks performed in this mode include setting the switch hostname, configuring passwords, defining VLANs, enabling routing protocols, and applying security settings. Commands issued in this mode apply globally unless overridden in a more specific configuration mode.

d) Interface configuration mode (Switch(config-if)#)

The Interface Configuration mode is a sub-mode of the Global Configuration mode and is used to configure individual switch ports or interfaces. This mode allows administrators to specify port settings such as speed, duplex mode, VLAN membership, port security, and IP address assignment for layer 3 interfaces. Commands in this mode only affect the selected interface. For example, one can configure FastEthernet0/1 with interface FastEthernet0/1 and then set its speed with speed 100 or assign it to VLAN 10 using switchport access vlan 10. Exiting this mode returns the user to Global Configuration mode.

VLANs and IP addressing

A virtual local area network (VLAN) segments a network logically to improve performance and security. VLAN 1 is the default VLAN for management unless changed. Each VLAN can be assigned an IP address to enable communication with other networks through a router or Layer 3 switch.

II.2 Simulation tool: Cisco Packet Tracer

Cisco Packet Tracer is a network simulation software developed by Cisco Systems [2]. It is designed to emulate networking devices such as routers, switches, and hubs. Its main purpose is to build virtual networks and simulate how different networking protocols behave. The user can design a topology using devices like switches, routers, and computers, and then interconnect them with different types of cables (copper, fiber, etc.). Once connected, the devices can be configured with parameters such as IP addresses, subnet masks, and network services, allowing learners to observe and test real networking behaviors in a safe, virtual environment.

III Practical part

III.1 Training implementation steps for topology 1

Topology 1: In this training, a small network will be set up consisting of a switch and a personal computer (PC). The devices will be connected using a straight-through cable, allowing students to configure the switch. Both the computer and the switch interface connected to it will be assigned IP addresses to enable communication, as illustrated in the network of Figure .1. On the other hand, Table .2 shows the topology addresses.

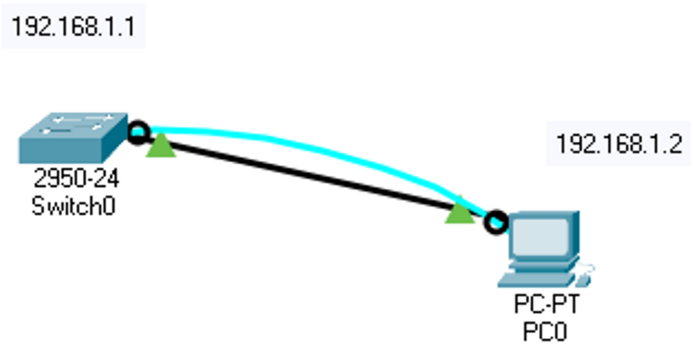

Figure .1: Simple topology of switch and PC

Table .2: Addressing table for topology 1

Device	**Interface**	**IP address**	**Subnet mask**
Switch	VLAN	192.168.1.1	255.255.255.0
PC	Network card	192.168.1.2	255.255.255.0

1. Go to Network Devices and click on Switch in the lower-left corner of the program, similar to previous exercises. Choose any Switch, drag it onto the workspace, and place it.

2. Next, go to End Devices, select a computer, and drag it onto the workspace.

3. Click Cable and choose Straight-Through. When connecting the computer to the switch, select Fast Ethernet for both devices.

4. In order to configure the computer, click on the computer, go to the desktop, and select IP Configuration.

5. Assign the IP address as shown in the following figure.

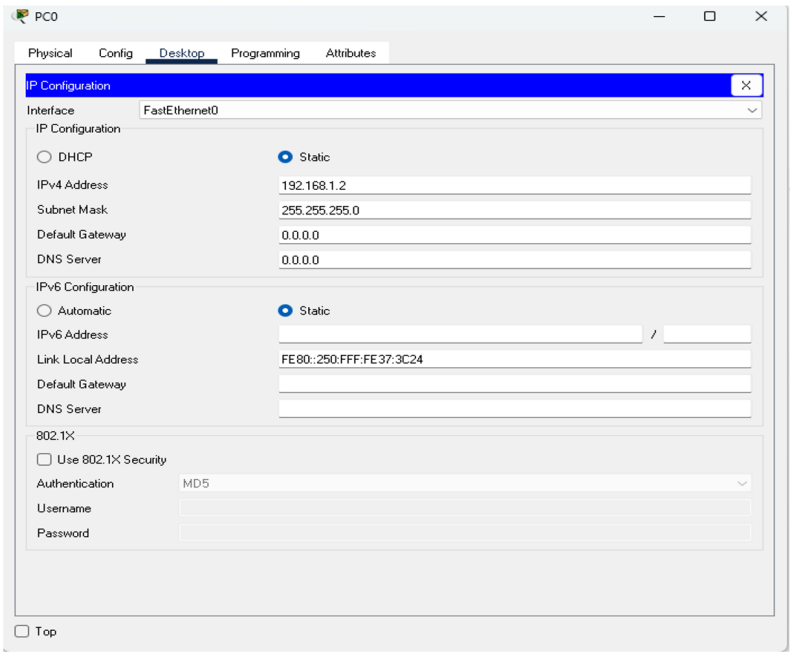

Figure .2: Assigning the IP address on PC

6. No, in order to set up the switch, click on the switch. Thereafter, select the command line interface called "CLI" (CLI: Command line interface), then type ‘Entre” so that the command line appears as follows.

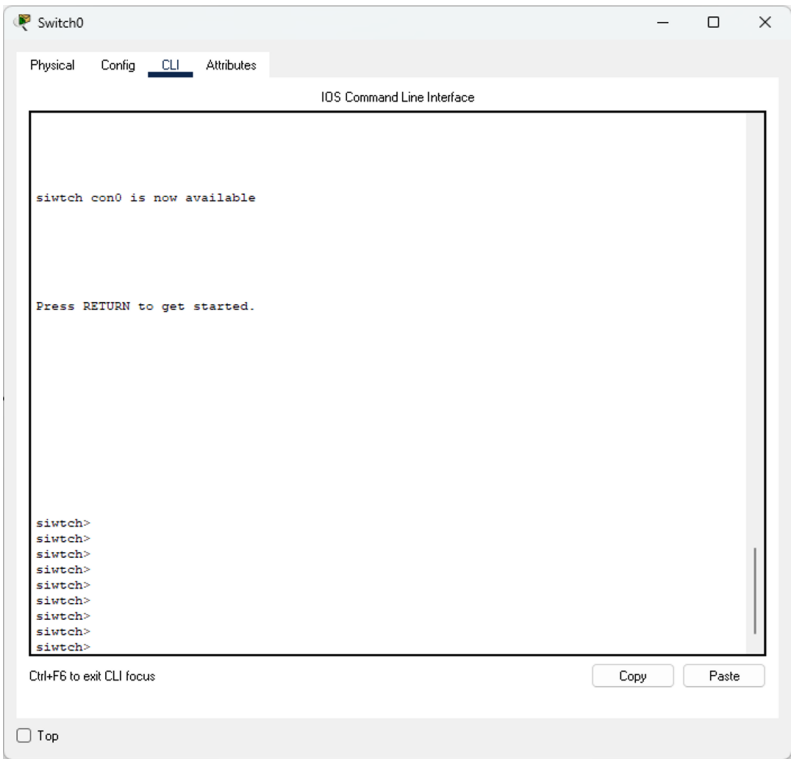

Figure .3: Switch login window

7. Now write the command enable command in order to transition from execution mode to privileged mode.

8. Type the command Switch#show running-config in order to display the current configuration of the switch.

   A. What is the hostname of the switch?
   B. How many Fast Ethernet interfaces does the switch have?
   C. How many Gigabit Ethernet interfaces does the switch have?
   D. What is the Spanning Tree mode used?
   E. What is the status of VLAN1? (Active or shutdown?)
   F. Is there an IP address assigned to VLAN1?
   G. How many VTY lines (virtual terminal lines) are configured?
   H. Is password encryption enabled on the switch?
   I. What is the current version of the internetwork operating system (IOS)?
   J. Which interfaces are listed in the configuration?

9. Now, delete the VLAN configuration file stored in the switch's flash memory to remove all VLANs using `delete flash:vlan.dat`. Before deleting, you must display existing VLANs using the command `show vlan brief`

   A. What is the default VLAN on a Cisco switch?

B. How many ports are currently assigned to the default VLAN?
C. What is the status of VLAN 1??
D. What are VLANs 1002 to 1005 used for?
E. How can you verify if a specific port belongs to a certain VLAN?

10. Deletes the startup configuration file from non-volatile RAM (NVRAM) using `Switch# erase startup-config`.

11. Restart (reboot) the switch using `reload` to apply configuration changes and clear deleted VLAN data from memory.

12. No use the command, `show startup-config` in order to display the configuration that is saved in the NVRAM, the configuration that will be loaded automatically when the switch starts or reloads.

    A. What does the message mean?
    B. Where is the startup configuration normally stored?
    C. Why might the startup-config be missing?

13. Next, save the current active configuration (`copy running-config startup-config`) stored in RAM to the startup configuration stored in NVRAM, so that it will be automatically loaded when the switch restarts, after use the command `show startup-config` in order to confirm that the configuration is saved.

    A. What is the difference between the commands `show startup-config` and `show running-config` on a cisco switch?

14. Now, type the `Switch#config terminal` command to make the required settings.

15. Change the name of the switch with the command `hostname`.

16. In order to configure an IP address on the switch referred to as a virtual IP address (for example, (`192.168.1.1`) along with the subnet mask (`255.255.255.0`), use the following commands. The interface is then activated with the no `shutdown` command to enable communication with the connected computer, as shown below:

```
Switch# configure terminal
Switch(config)# hostname Switch1
Switch(config)# interface vlan1
Switch1(config-if)# ip address 192.168.1.1 255.255.255.0
Switch1(config-if)# no shutdown
```

17. No return to the previous settings, use the exit command as follows:

```
Switch1(config-if)# exit
Switch1(config)# exit
```

18. In order to verify that the switch has the correct IP address configured, enter the following command `show running-config`, thereafter use the command, `show interface vlan1` in order to display information about the management interface (VLAN 1) on a Cisco switch.

    A. What command is used to display the status of VLAN 1?
    B. What does "Vlan1 is administratively down, line protocol is down" mean?
    C. What type of interface is VLAN 1?
    D. What is the MTU of the VLAN 1 interface?
    E. Why is there no traffic on VLAN 1?
    F. How can you activate VLAN 1 and make it ready for remote management?

19. Connect the PC to the switch using one of the FastEthernet ports (you can choose any port from FastEthernet 0/1 to FastEthernet 0/24). Then, exit the Privileged EXEC Mode and use the command `show interface fastethernet 0/x` in order to display the status and statistics of the selected port.

    A. What is the purpose of the command `show interface fastethernet 0/1`?
    B. What does the line `FastEthernet0/x is up, line protocol is up` mean?
    C. What is the meaning of `Full-duplex, 100Mb/s`?
    D. What is the MAC address?
    E. What does `Keepalive set (10 sec)` mean?
    F. What can you conclude if the interface is down/down instead of up/up?

20. Let's examine the switch memory by using the following command: Erase the initial configuration file from the switch's NVRAM (factory reset style) by using this command `Switch1#dir flash`.

    A. What is the file Cisco IOS image file?
    B. What does the file `config.text represent`?
    C. What is total memory capacity of the flash and the available free space remaining of the switch?

21. After you delete `flash:vlan.dat` and reload the switch, you can verify that the VLAN configuration has been reset using the command `Switch# show vlan brief`.

22. Finally, save the current active configuration (`copy running-config startup-config`) stored in RAM to the startup configuration stored in NVRAM.

III.2 Training implementation steps for topology 2

Topology 2: As we knew the switch operates at Layer 2 in the OSI model, which means it typically does not require an IP address. However, to access the switch's interface remotely from a computer, it must be assigned an IP address, known as a virtual IP address.

Telnet command: Telnet is both a protocol and an application that allows users to log into a remote device, such as a switch or router. It enables the user to execute commands on the remote device as if they were working locally. In this practical work, a small network will be set up consisting of two switches connected together and two computers as shown in Figure .4. The network will be arranged so that students can access the switches' configuration pages. IP addresses will be assigned to the computers and the connected switch interfaces to enable communication, as illustrated in the following network diagram.

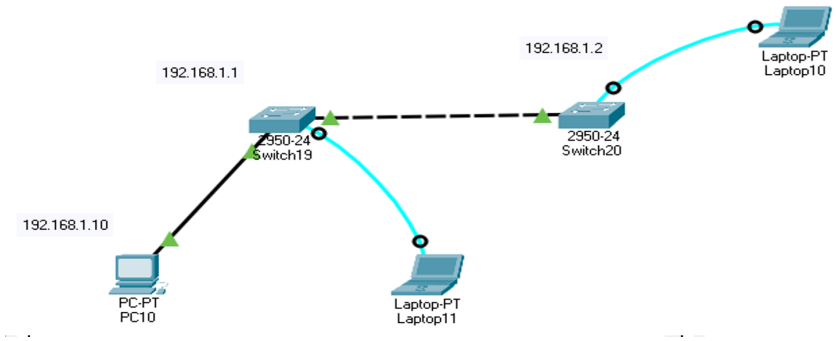

Figure .4: Topology of 2 switch and 1 PC

1. In the bottom-left corner of the program, click on "Switch", then choose two switches and place them onto the workspace.

2. Go to "End Devices", pick one computer and two laptops, and drag them onto the workspace as done in the previous exercises.

3. Select "Cable" and choose "Crossover". Use it to connect the two switches by linking their Fast Ethernet ports.

4. Again, click on "Cable", but this time choose "Straight-Through" to connect the first computer to the first switch, using the Fast Ethernet ports on both devices.

5. Finally, select "Cable" and pick "Console" to configure the switch. Connect the second switch to the second computer using the Console port on the switch and the RS232 serial port on the computer.

6. Access the Switch and open its home page using the control cable (Console) as follows:

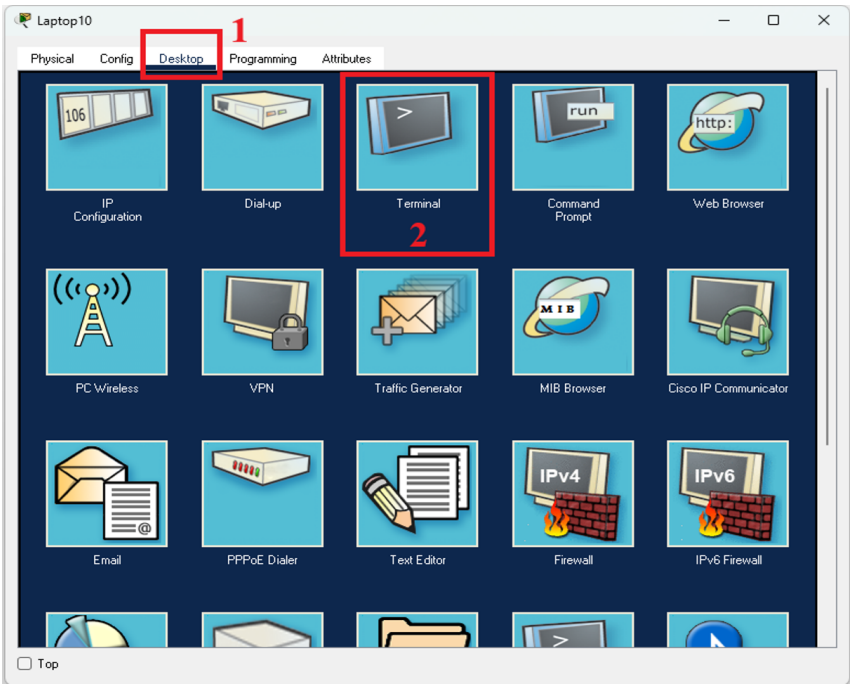

Figure .5: Access to switch via console laptop

7. After entering the switch page, basic settings are made, such as assigning a virtual Internet Protocol (VLAN IP) address for the switch and creating its password as follows:

   For switch 1 related to the fixed PC (same steps for switch 2) configuration:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

8. Now use the command `line vty 0 x` in order to enter the configuration mode for the virtual terminal (VTY) lines, which are responsible for remote access to the switch via Telnet or SSH.

   - `vty` stands for Virtual Teletype, meaning virtual command-line sessions.
   - `0 x` indicates five VTY lines (from line 0 to line x)

```
Switch(config)# line vty 0 4
Switch(config-line)# password cisco1
Switch(config-line)# login
```

9. The command `transport input telnet` specifies which remote access protocols are allowed on the VTY lines.

```
Switch(config-line)# transport input telnet
Switch(config-line)# exit
Switch(config)# end
Switch# write memory
```

10. After making the switch configurations, now it should make a remote connection using the telnet command from the fixed computer connected to the switch via a straight-through cable to the switch's IP address, as shown in the following Figure.

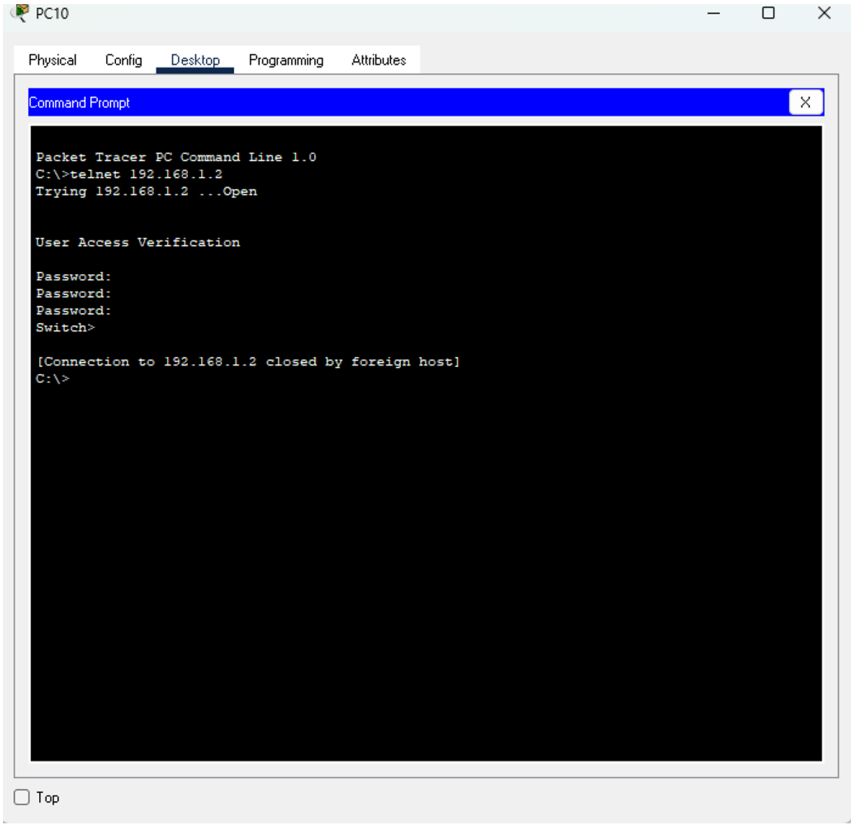

Figure .6: Remote connection using the telnet

11. What are your comments?

Conclusion

This PW provided hands-on experience with the basic configuration and management of Cisco switches in a local area network environment. Through the use of Cisco Packet Tracer, the fundamental role of a switch at Layer 2 of the OSI model was explored, along with its capability to support management and remote access through logical interfaces.

In the first topology, the essential steps for initial switch configuration were performed, including accessing the device through the console, examining the default parameters, erasing existing configurations, and understanding the difference between running and starting configurations. The configuration of a management IP address on VLAN 1 enabled basic communication with a connected PC, allowing verification of connectivity and interface status. These steps highlighted the importance of proper switch initialization, memory management, and interface activation for reliable network operation.

In the second topology, remote management concepts were introduced using Telnet. By configuring virtual terminal (VTY) lines and assigning appropriate IP addresses, remote access to the switch was successfully established. This demonstrated how switches, although mainly Layer 2 devices, can be remotely managed once a management interface is configured. The experiment also emphasized the role of cabling types, interface states, and security considerations related to remote access.

This PW strengthened the understanding of Cisco switch operation, configuration modes, VLAN management, and basic network troubleshooting. The acquired skills form a solid foundation for more advanced topics such as VLAN segmentation, inter-VLAN routing, switch security, and the use of secure remote access protocols in real network environments.

PW2: Creation and configuration of a VLAN-segmented network

I Learning Objectives

In this practical work, the student learns about the purpose of VLANs in a switched network. The main objectives are:

Part 1: Basic switch configuration

- To understand the role of a Cisco switch in a local area network (LAN).
- To learn and apply the fundamental configuration commands of a switch.
- To configure basic device settings such as hostname and console/VTY access.
- To verify and analyze switch interfaces and status using diagnostic commands.
- To save and manage configuration files in the switch memory (NVRAM/Flash).

Part 2: VLAN configuration and network segmentation

- To create and configure VLANs on Cisco switches.
- To assign ports to VLANs by configuring them in Access mode.
- To configure inter-switch communication using Trunk mode.
- To understand how VLANs improve network organization, security, and traffic management.
- To test connectivity between hosts in the same VLAN and isolation between different VLANs.

II Theoretical Background

II.1 VLAN Definitions

Imagine you are organizing a massive conference that hosts participants from different places and fields of interest. Among them are specialists who need to share their knowledge with smaller, focused groups. If all of these experts tried to speak in one large hall at the same time, the result would be total confusion; no one would be able to clearly follow any presentation. To solve this, you would divide the participants into separate rooms so that each expert can communicate effectively with their audience [5].

This is exactly what a VLAN does within a computer network. A VLAN is implemented at Layer 2 to segment a large network into smaller, more manageable virtual networks. This separation reduces unnecessary broadcast traffic and improves performance. Devices within the same VLAN can communicate directly with each other, while being isolated from traffic in other VLANs. Network administrators can create VLANs based on location, department, type of equipment, or any other relevant criteria. Learning how to configure VLANs is essential for structuring efficient and secure modern networks [5].

Dividing a network into smaller segments is more complex than simply sorting screws into separate containers, yet doing so greatly improves network control and efficiency. VLANs make this possible by logically dividing a switched network into separate sections. Devices that belong to the same VLAN can communicate with each other as though they were connected to the same physical cable, even if they are not. Unlike traditional networks that rely on physical layout, VLANs use logical grouping. This means that employees from different departments, such as IT, Human Resources, or Sales, can be part of the same network segment even if they are connected to different switches or located in separate areas of a campus network, as shown in Figure .1.

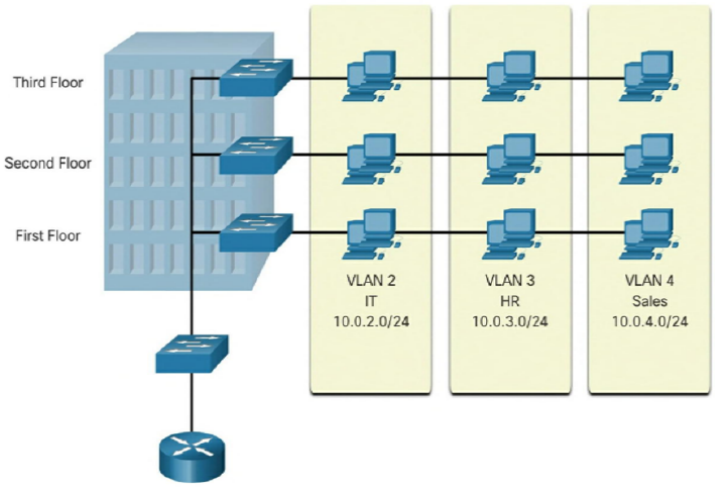

Figure .1: VLAN groups [6]

With VLANs, network administrators can divide a network into separate segments according to criteria such as department, role, or specific application needs, regardless of where users or devices are physically located. Each VLAN functions as an independent logical network. Devices assigned to the same VLAN communicate as though they are part of a standalone network, even though they may share the same physical switching hardware with other VLANs. Additionally, any switch port can be configured to join a VLAN, providing flexibility in network design and management [5].

II.2 Types of VLANs

VLANs are used to logically divide a physical network into multiple separate broadcast domains. This segmentation improves security, reduces unnecessary traffic, and simplifies network management. Depending on how devices are grouped and assigned to VLANs, different classification methods can be used. These methods operate at different layers of the OSI model and determine how a switch decides which VLAN a device belongs to. The main types of VLANs are classified as follows:

- **Level 1 VLAN (Port-based VLAN):** This is the simplest type of VLAN. Each switch port is manually assigned to a specific VLAN. Any device connected to that port automatically becomes a member of the assigned VLAN. This method is easy to configure and is widely used in enterprise networks.
- **Level 2 VLAN (MAC-based VLAN):** In this type, VLAN membership is determined by the MAC address of the device rather than the physical port. The switch examines the source MAC address of incoming frames and assigns them to the appropriate VLAN according to a predefined MAC-to-VLAN mapping table, often managed by a server. This provides more flexibility when users move to different ports, as they remain in the same VLAN.
- **Level 3 VLAN (IP-based VLAN):** Here, classification into VLANs is based on the source IP address of received packets. The switch uses Layer 3 information to decide which VLAN a device belongs to. This method allows more dynamic network management but requires more advanced configuration.

II.3 Defining VLAN Trunks

In a switched network that uses VLANs, devices belonging to the same VLAN may be connected to different switches. To allow these VLANs to communicate across multiple switches, a special type of link called a VLAN trunk is used (Figure .2). A trunk is a point-to-point connection that carries traffic from multiple VLANs over a single physical link between switches, routers, or servers. Unlike access ports, which transport traffic for only one VLAN, trunk ports

use tagging methods such as IEEE 802.1Q to identify the VLAN each frame belongs to. This enables efficient VLAN communication across an extended network infrastructure while preserving VLAN separation.

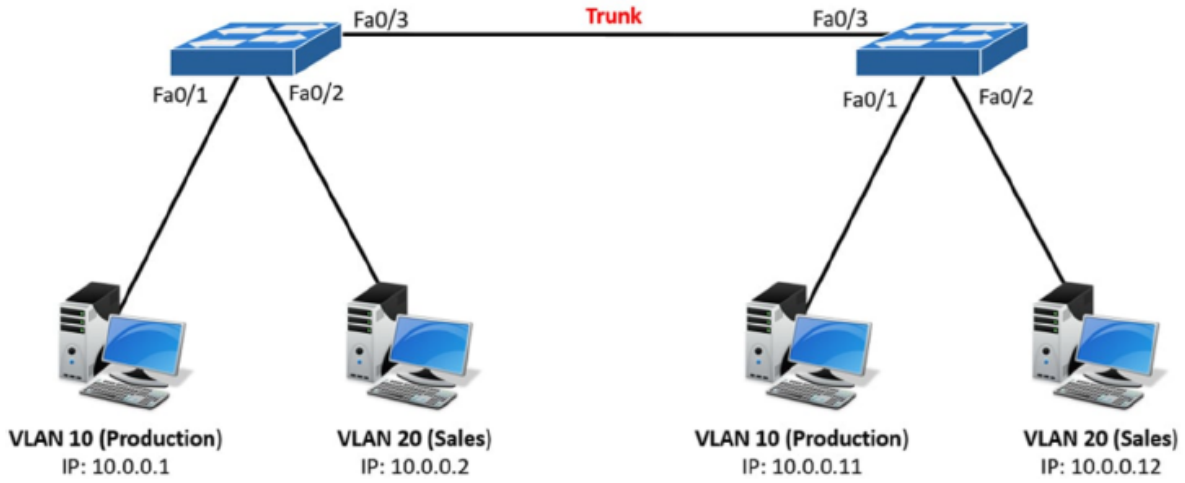

Figure .2: VLAN trunk [6]

II.4 Network without VLANs

In a traditional network that does not use VLANs, all devices connected to a switch belong to the same broadcast domain, as shown in Figure .3. This means that any broadcast message sent by one device is forwarded to every other device on the network, regardless of their department, role, or purpose.

While this type of flat network architecture is simple to implement, it becomes inefficient and difficult to manage as the number of devices increases. Without VLANs, there is no logical separation of traffic, which can lead to issues such as network congestion, security vulnerabilities, and a lack of traffic control.

For example, sensitive data from the finance department might share the same network as public guest traffic, increasing the risk of data breaches. Additionally, troubleshooting becomes more challenging, as broadcast traffic and unnecessary communication between unrelated devices can degrade overall network performance. For these reasons, modern networks rarely operate without segmentation provided by VLANs.

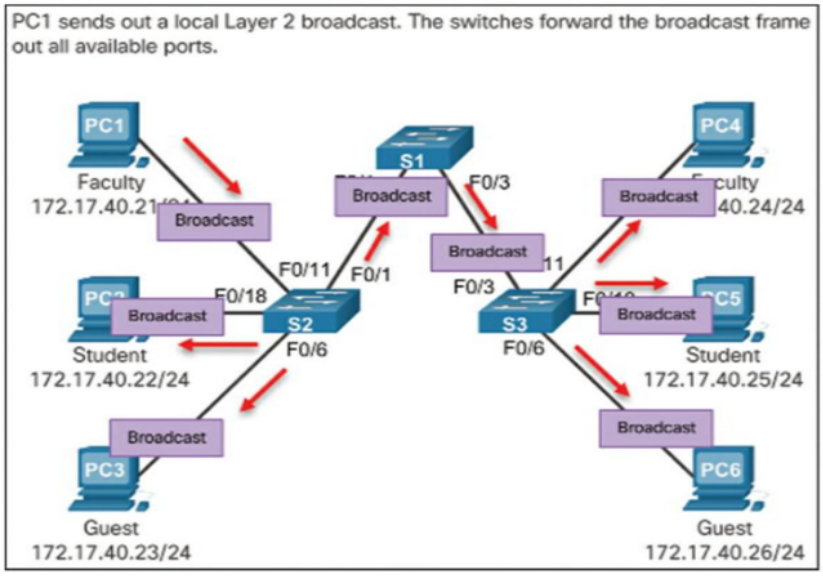

Figure .3: Broadcast domain without VLAN [7]

II.5 Network with VLANs

VLANs are created and applied to specific switch ports, and any device connected to those ports automatically becomes part of the corresponding VLAN. End devices themselves do not recognize the concept of VLANs; they simply operate using their assigned IP addresses and subnet configurations.

This is where the relationship between a VLAN and an IP network becomes clear: each VLAN represents a separate logical subnet. While VLAN configuration is handled on the switch, IP addressing is set directly on the connected devices.

As shown in Figure .4, in a network divided into two VLANs, such as VLAN 10 for faculty and VLAN 20 for students, each group is isolated at Layer 2. If a broadcast is sent from a faculty computer connected to VLAN 10, the frame will remain within that VLAN and will only be forwarded to other devices that belong to VLAN 10. Even though the diagram may show trunk connections between switches, traffic does not cross from one VLAN to another unless routing is explicitly configured.

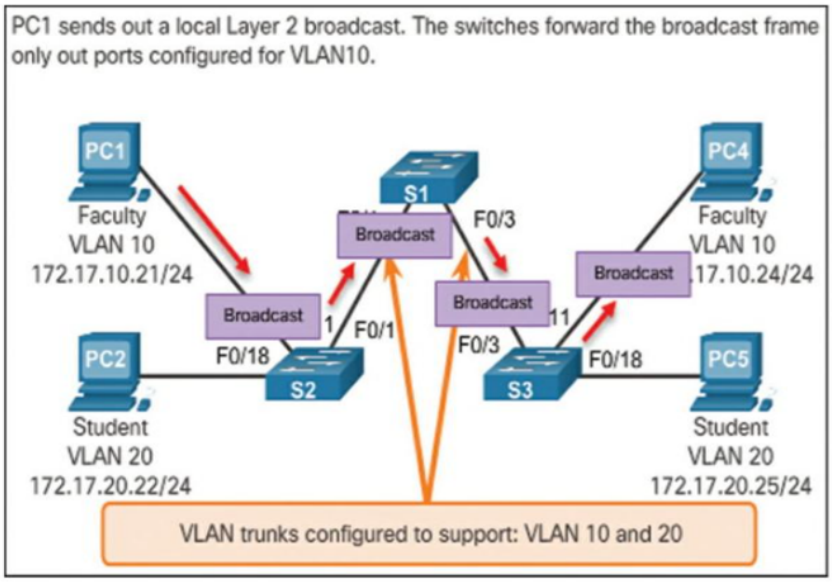

Figure .4: Broadcast domain with VLAN [7]

II.6 VLAN identification with a tag

When VLANs are used in a network, frames must carry information that identifies the VLAN they belong to, especially when they travel across trunk links. This is achieved through a process called VLAN tagging. VLAN tagging is a method used to insert a small piece of information, known as a tag, inside the Ethernet frame. This tag specifies the VLAN ID (ranging from 1 to 4094) to which the frame belongs. The most widely used tagging standard is IEEE 802.1Q. With 802.1Q tagging, a 4-byte header is inserted into the Ethernet frame just after the source MAC address as presented in Figure .5. This header contains the VLAN Identifier (VID), which allows switches to correctly forward traffic to the appropriate VLAN across trunk links. When the frame reaches its destination switch or access port, the tag is removed before being delivered to the end device. This ensures that VLAN tagging is invisible to hosts and only used by network switches for traffic management. The VLAN tagging is essential in maintaining separate broadcast domains over a shared physical link while still enabling multiple VLANs to communicate through trunk connections [6].

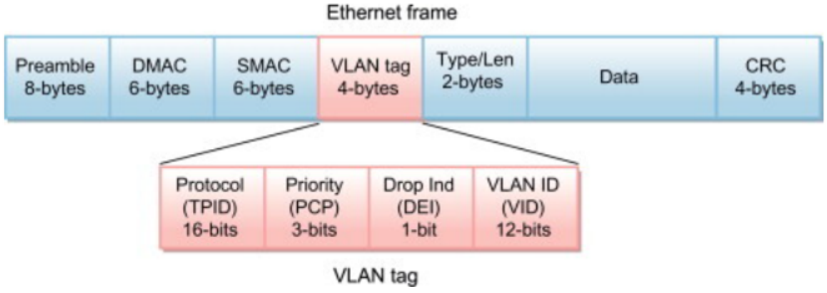

Figure .5: Fields in an Ethernet 802.1Q frame [7]

III Practical part

III.1 Training-related knowledge for topology 1

Topology 1: In this training, a small network (Level 1) will be set up consisting of 1 switch (Cisco 2960) and 2 computers as shown in Figure .6. The goal is to assign PC1 to VLAN 10 and PC2 to VLAN 20, ensuring each VLAN functions as a separate network. First, open Cisco Packet Tracer and create the topology by dragging one switch and two PCs onto the workspace. Connect PC1 to the switch port FastEthernet0/1 and PC2 to FastEthernet0/2. Next, configure the IP addresses on the PCs as shown in Table .1.

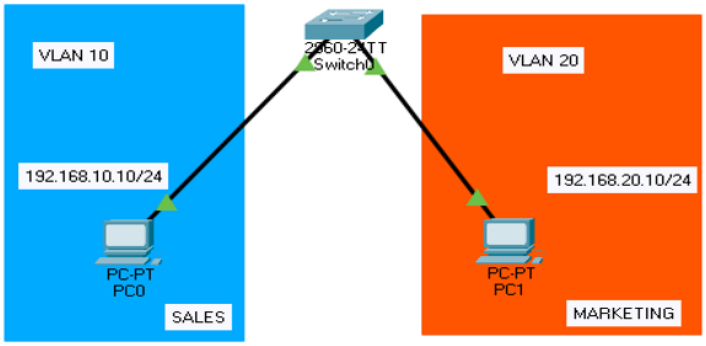

Figure .6: Small network with 2 VLANs

Table .1: Addressing table for topology 1

PC	Switch port	VLAN	IP address	VLAN name	Subnet mask
PC1	Fa0/1	10	192.168.10.10	SALES	255.255.255.0
PC2	Fa0/2	20	192.168.20.10	MARKETING	255.255.255.0

1. Create the topology by opening Cisco Packet Tracer. Drag: 1 switch (e.g., 2960-24TT) and 2 PCs. Connect PC1 to switch port FastEthernet0/1 and PC2 to switch port FastEthernet0/2.

2. Assign the IP address and subnet to each PC using Table .1.

3. Change the name of the switch to SW1.

4. Configure the VLANs on the switch using the CLI:

```
SW1> enable
SW1# configure terminal
SW1(config)# vlan 10
SW1(config-vlan)# name SALES
SW1(config-vlan)# exit
```

```
SW1(config)# vlan 20
SW1(config-vlan)# name MARKETING
SW1(config-vlan)# exit
```

5. Assign switch ports to VLANs:

```
SW1(config)# interface fastEthernet 0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# exit

SW1(config)# interface fastEthernet 0/2
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20
SW1(config-if)# exit
```

6. Verify VLAN configuration using the command `show vlan brief` and write the execution results.

7. Test connectivity using the `ping` command from PC1 to PC2. Observe the results and explain the reason. Conclude your observations.

III.2 Training-related knowledge for topology 2

Topology 2: Now configure 6 PCs connected to one switch, and group them into 3 VLANs, but not in a simple order (they're mixed) as shown in Figure .7. Scenario setup and configuration IP addresses of this topology are shown in the Table .2:

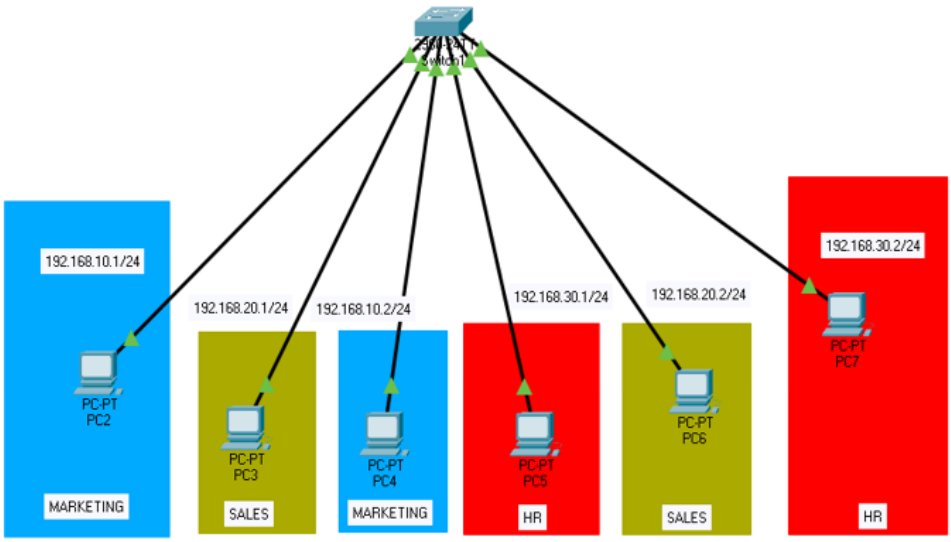

Figure .7: Mixt network with 3 VLANs

Table .2: Addressing table for topology 2

PC	Switch port	VLAN	IP address	VLAN name	Subnet mask
PC1	Fa0/1	10	192.168.10.1	MARKETING	255.255.255.0
PC2	Fa0/2	20	192.168.20.1	SALES	255.255.255.0
PC3	Fa0/3	10	192.168.10.2	MARKETING	255.255.255.0
PC4	Fa0/4	30	192.168.30.1	HR	255.255.255.0
PC5	Fa0/5	20	192.168.20.2	SALES	255.255.255.0
PC6	Fa0/6	30	192.168.30.2	HR	255.255.255.0

1. Create the topology and configure the IP addresses on all PCs as per Table .2.
2. Access the switch CLI and configure VLANs and assign ports to VLANs, similar to the previous example.
3. Verify VLAN configuration using the command `show vlan brief` and record the output.
4. Now, test connectivity:
   - From PC1, ping PC3.
   - From PC1, ping PC2.
   - From PC4, ping PC6.
   - From PC5, ping PC3.

   Observe the results and explain why certain pings succeed and others fail.

III.3 Training-related knowledge for topology 3

Topology 3: Now, in this topology, go with two switches connected with a trunk link so VLANs can work across both switches. This is a level 2 VLAN with trunking, but VLANs can communicate between PCs on different switches that belong to the same VLAN. The network setup is shown in the Table .3:

Table .3: The network setup for topology 3

VLAN	Name	Network	PCs (Switch:Port)
10	MARKETING	192.168.10.0/24	PC1 (SW1-Fa0/1), PC3 (SW2-Fa0/3)
20	SALES	192.168.20.0/24	PC2 (SW1-Fa0/2), PC5 (SW2-Fa0/4)

In order to create a trunk connection between two switches, we will use two Cisco 2960 switches and four PCs, with two PCs connected to each switch. In Cisco Packet Tracer, begin by building the topology. Connect PC1 to switch1 on port FastEthernet0/1 and PC2 to switch1 on port FastEthernet0/2. Then, connect PC3 to Switch2 on port FastEthernet0/3 and PC4 to Switch2 on port FastEthernet0/4. Finally, establish a trunk link between the two switches by

connecting switch1's FastEthernet0/24 port to Switch2's FastEthernet0/24 port. The proposed topology and its configuration are presented in Figure .8 and Table .4, respectively.

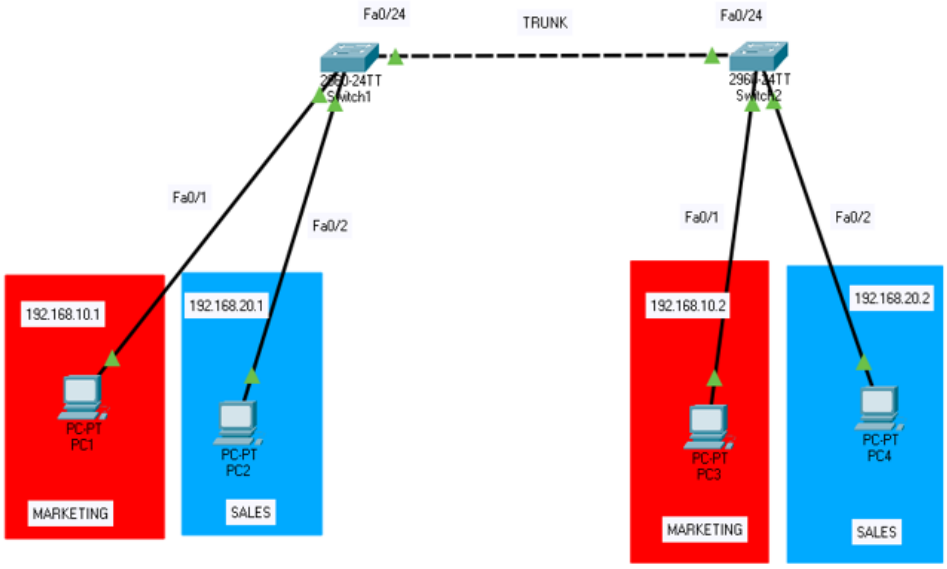

Figure .8: Two switches with trunk

Table .4: Addressing table for topology 3

PC	VLAN	IP Address	Subnet Mask
PC1	10	192.168.10.1	255.255.255.0
PC2	20	192.168.20.1	255.255.255.0
PC3	10	192.168.10.2	255.255.255.0
PC4	20	192.168.10.2	255.255.255.0

1. Create the topology and configure IP addresses on PCs as in Table .4.
2. Connect two switches (SW1 and SW2) using a trunk link so that VLANs are extended across both switches. This allows PCs in the same VLAN (even on different switches) to communicate.
3. Configure VLANs on both switches using the following commands:

```
Switch> enable
Switch# configure terminal
% Create VLAN 10 and 20
Switch(config)# vlan 10
Switch(config-vlan)# name MARKETING
Switch(config-vlan)# exit
Switch(config)# vlan 20
```

```
Switch(config-vlan)# name SALES
Switch(config-vlan)# exit
```

4. Assign ports to VLANs as in the previous examples.

5. Configure the trunk link on both switches using the following commands:

```
Switch1(config)# interface fa0/24
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan 10,20
Switch1(config-if)# exit
```

6. Verify VLAN configuration using the command `show vlan brief` on both switches. Write the execution results.

7. Test the connectivity:

   - PC1 to PC3
   - PC2 to PC4
   - PC1 to PC2

   Note the results and explain the reason for successful or failed communication.

Conclusion

In this PW, students gained comprehensive experience in creating and managing VLAN-segmented networks using Cisco switches. The exercises emphasized both the theoretical and practical aspects of VLANs, including their purpose in logically dividing a network, reducing broadcast traffic, improving security, and facilitating efficient network management.

Through the first topology, students learned to configure basic switch settings, assign VLANs to individual ports, and verify network segmentation using diagnostic commands. The second topology extended this knowledge to more complex scenarios, demonstrating how multiple VLANs can coexist on a single switch and how connectivity is restricted between devices in different VLANs. Finally, the third topology introduced trunking between switches, enabling VLANs to span multiple devices while maintaining logical separation of broadcast domains.

These exercises reinforced the importance of VLAN planning, proper IP addressing, and port assignment in achieving network organization and isolation. Students also developed skills in testing and troubleshooting network connectivity, observing how VLAN configurations directly impact communication between hosts.

This PW provided a solid foundation for understanding VLAN operation, inter-switch communication, and network segmentation techniques, preparing students for more advanced network design and administration tasks in enterprise environments.

PW3: Configuration of inter-VLAN routing. Simulation using Packet Tracer or practical work on real platforms.

I Learning objectives

By the end of this practical work, the student will be able to:

- Understand the concept of a multilayer switch (Layer 3 switch) and explain how it combines both switching and routing functionalities in a single device.
- Differentiate between Layer 2 switching and Layer 3 routing, and describe how inter-VLAN communication is achieved without using an external router.
- Create and configure VLANs on a multilayer switch to logically segment a network into different departments or groups.
- Configure switched virtual interfaces (SVIs) and assign IP addresses to provide Layer 3 connectivity between VLANs.
- Enable and verify Layer 3 routing using the `ip routing` command to allow communication between VLANs.
- Assign ports to specific VLANs and test network connectivity using basic troubleshooting commands such as `ping`, `show ip interface brief`, and `show vlan brief`.
- Analyze the benefits of using a multilayer switch compared to the *router-on-a-stick* method in terms of performance, scalability, and design simplicity.

II Theoretical background

II.1 Inter-VLAN routing

In modern computer networks, VLANs are used to divide a single physical network into several logical networks. Each VLAN behaves as a separate network, which improves security, organization, and traffic management. However, this separation also means that devices in different VLANs cannot communicate directly. For example, computers in VLAN 10 cannot send data

to computers in VLAN 20. In order to allow communication between VLANs, a process called **Inter-VLAN routing** is required [6].

II.2 Router-on-a-stick concepts

The router-on-a-stick is a common and cost-effective method used to perform inter-VLAN routing, allowing communication between different VLANs in a network (Figure .1). In this configuration, a single physical interface on a router is connected to a switch. Instead of dedicating one interface per VLAN, the router interface is divided into multiple logical subinterfaces, one for each VLAN.

The link between the switch and the router is configured as a trunk link, which carries traffic from multiple VLANs over a single physical connection. Each subinterface is assigned a unique IP address that serves as the default gateway for the corresponding VLAN.

When a device in one VLAN needs to communicate with a device in another VLAN, its traffic is sent to the router through the trunk link. The router uses the IEEE 802.1Q tagging protocol to identify the VLAN, routes the packet to the appropriate destination VLAN, and sends it back through the same trunk link.

This technique simplifies inter-VLAN communication by requiring only one physical connection between the switch and the router, making it an efficient solution for small to medium-sized networks. However, it can also create a bottleneck because all inter-VLAN traffic must pass through a single link, which may affect multiple active paths exist.

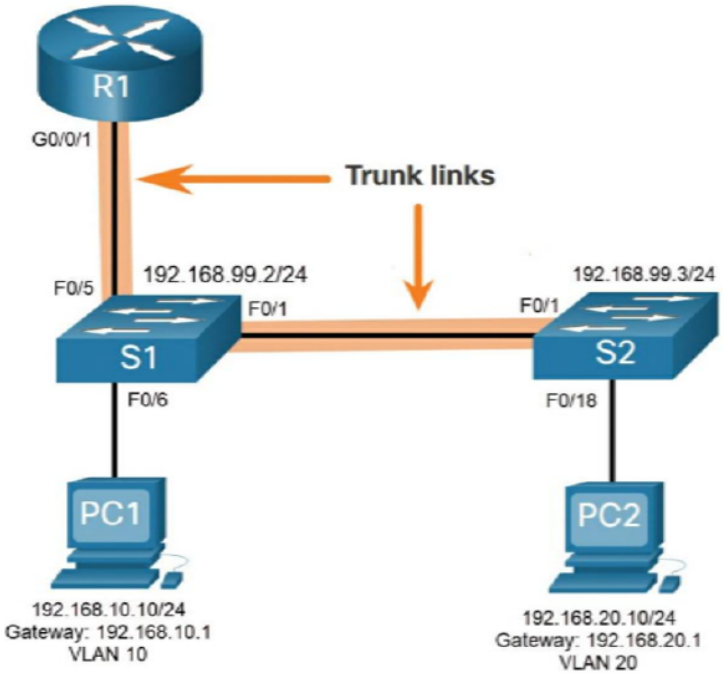

Figure .1: Router-on-a-stick topology [7]

II.3 Inter-VLAN routing using Layer 3 switches

A multilayer switch is a network device that combines the high-speed performance of a Layer 2 switch with the routing capabilities of a router. Unlike traditional Layer 2 switches that only forward frames based on MAC addresses, a Layer 3 switch can make routing decisions using IP addresses, allowing communication between different VLANs directly within the switch.

This process, known as **Inter-VLAN routing**, eliminates the need for an external router, thereby reducing latency and improving overall network efficiency. Layer 3 switches use **switched virtual interfaces (SVIs)** to assign IP addresses to VLANs, with each SVI acting as the default gateway for devices within the corresponding VLAN.

By enabling the `ip routing` command, the switch performs routing between VLANs internally, providing faster and more scalable network performance. This makes multilayer switches ideal for enterprise and campus networks that require both switching and routing functions within a single device.

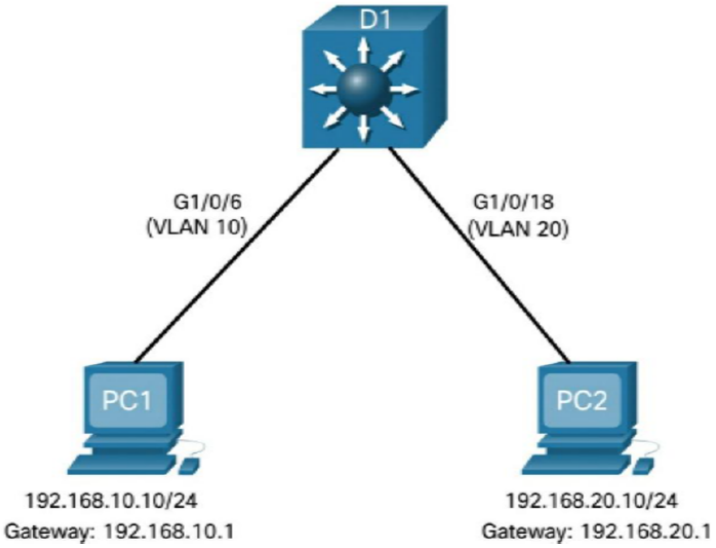

Figure .2: Inter-VLAN routing using layer 3 switches topology [7]

II.4 Why inter-VLAN routing is important

Inter-VLAN routing plays a crucial role in modern network design for several reasons:

- It allows communication between different departments (e.g., Accounting $\leftrightarrow$ HR).
- It uses only one router port, which helps save hardware resources.
- It is a fundamental concept in network design and an essential topic for CCNA certification and network engineering. Table .1 summarizes the Inter-VLAN routing advantages and disadvantages.

Table .1: Inter-VLAN routing advantages and disadvantages

Advantages	**Disadvantages**
Simple and inexpensive	Creates a traffic bottleneck on a single link
Requires only one physical router port	Not ideal for very large or high-traffic networks
Easy to understand and configure	Depends heavily on router performance

III Practical part

III.1 Training-related knowledge for topology 1

Topology 1: This training focuses on a simple and clear *router-on-a-stick* configuration using Cisco Packet Tracer. The topology consists of one switch, one router, and two computers, as illustrated in Figure .3.

The objective of this configuration is to assign **PC1** to **VLAN 10** and **PC2** to **VLAN 20**, ensuring that each VLAN operates as an independent network while still allowing inter-VLAN communication through the router.

To begin, open Cisco Packet Tracer and create the topology by placing one switch, one router, and two PCs in the workspace. Connect:

- PC1 to the switch on interface `FastEthernet0/1`
- PC2 to the switch on interface `FastEthernet0/2`
- The router to the switch on interface `FastEthernet0/3`

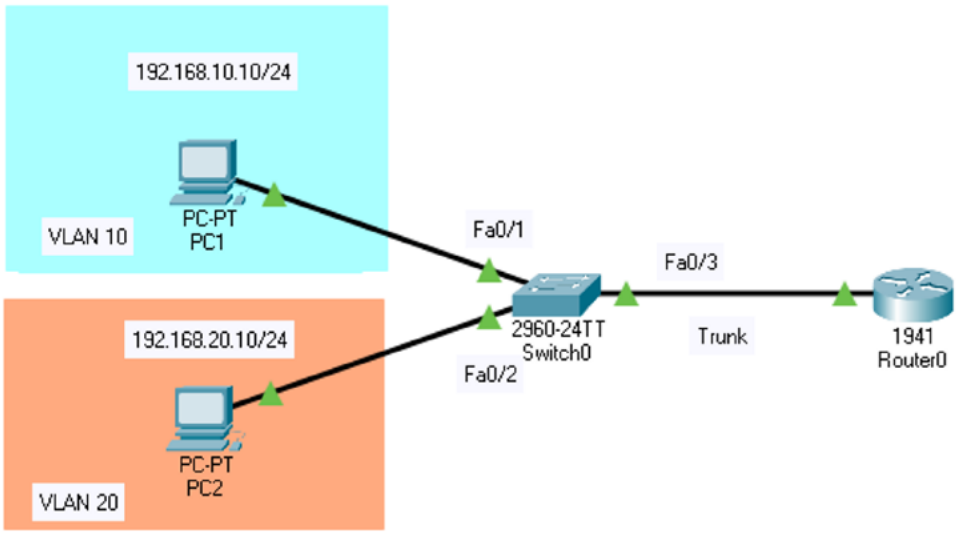

Figure .3: Simple configuration of router-on-a-stick

Next, configure the IP addresses on the PCs as shown in Table .2.

Table .2: IP addressing scheme for router-on-a-stick configuration.

Device	VLAN	IP Address	Subnet Mask	Gateway
PC1	VLAN 10	192.168.10.10	255.255.255.0	192.168.10.1
PC2	VLAN 20	192.168.20.10	255.255.255.0	192.168.20.1

1. Configure VLANs on the switch:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name SALES
Switch(config-vlan)# exit
% Repeat the same steps for VLAN 20
% Assign ports to VLANs
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
% Repeat the same steps for VLAN 20
% Configure the trunk to the router
Switch(config)# interface fa0/3
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

2. Configure router subinterfaces:

```
Router> enable
Router# configure terminal
% Enable main interface
Router(config)# interface gig0/0
Router(config-if)# no shutdown
Router(config-if)# exit
% Subinterface for VLAN 10
Router(config)# interface gig0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
% Subinterface for VLAN 20
% Repeat same steps for VLAN 20
```

3. Verify the configuration: Use the following commands:
   - Router: `show ip interface brief`
   - Switch: `show vlan brief` and `show interfaces trunk`
4. Test the connectivity using Ping from PC1 to PC2 and PC2 to PC1. Observe the results and explain any behavior.
5. What is the default gateway for VLAN 10 and VLAN 20 in this example?

III.2 Training-related knowledge for topology 2

Topology 2: In this topology, let's configure an inter-VLAN routing using a Layer 3 switch in order to enable communication between different VLANs within the same network. Let's create two VLANs: VLAN 10 for the sales department and VLAN 20 for the HR department, and assign each group of PCs to its corresponding VLAN as shown in Figure .4. Then, let's configure SVIs for each VLAN, providing an IP address that serves as the default gateway. After enabling the IP routing feature on the switch, let's verify that devices in different VLANs can communicate with each other successfully. This exercise demonstrates how a Layer 3 switch can perform both switching and routing functions, allowing efficient inter-VLAN communication without the need for an external router. The IP addresses on the PCs as shown in Table .3:

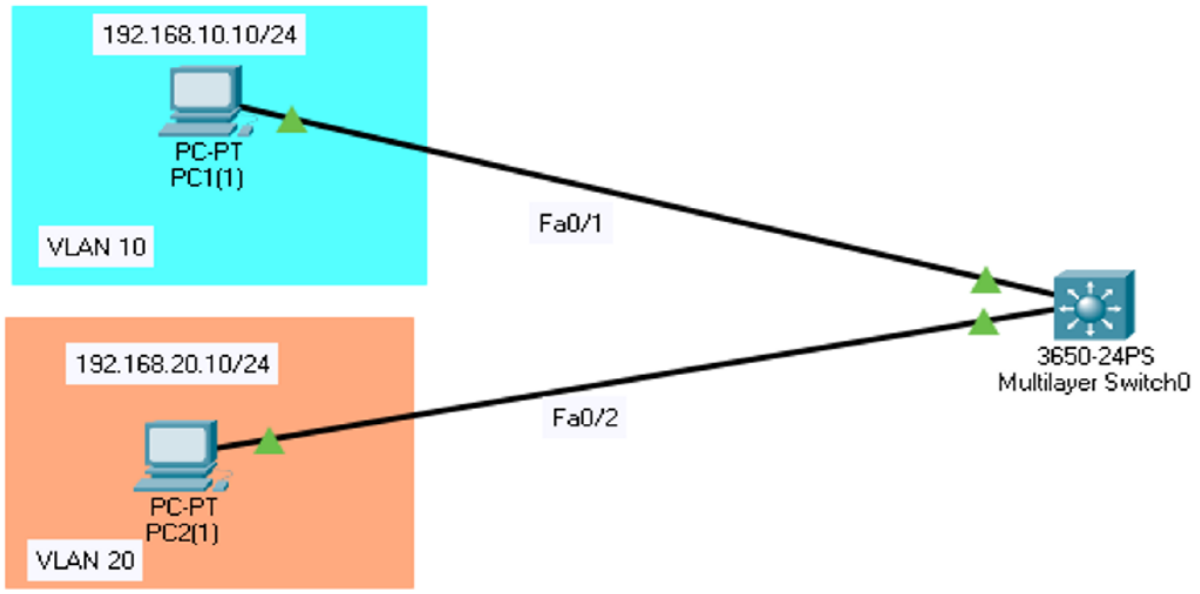

Figure .4: Layer 3 switch inter-VLAN Routing

Table .3: Addressing table for topology 2.

Device	VLAN	IP Address	Subnet Mask	Gateway
PC1	VLAN 10	192.168.10.10	255.255.255.0	192.168.10.1
PC2	VLAN 20	192.168.20.10	255.255.255.0	192.168.20.1

1. First go to switch and configure the VLANs using the following command:

```
Switch> enable
Switch# configure terminal

% Create VLANs
Switch(config)# vlan 10
Switch(config-vlan)# name SALES
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name HR
Switch(config-vlan)# exit

% Assign ports to VLANs
Switch(config)# interface gigabitEthernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
% Same steps for VLAN 20
```

2. Create SVI interfaces for routing:

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
% Same steps for VLAN 20

% Enable Layer 3 routing
Switch(config)# ip routing
```

3. Verify VLAN configuration using the command `show ip interface brief`. Write the execution results.

4. Test the connectivity using the `ping` command from PC1 to PC2 and PC2 to PC1. Observe the results, and explain what you notice and why.

III.3 Training-related knowledge for topology 3

Topology 3: In this topology, let design configuration for a lab: one Layer-3 switch (MLS) connected to two Layer-2 switches as shown in Figure .5. It includes a topology diagram, VLAN/IP plan, exact CLI commands for the MLS and both L2 switches, PC assignments, verification steps, and test questions. The IP addresses on the PCs as shown in Table .4:

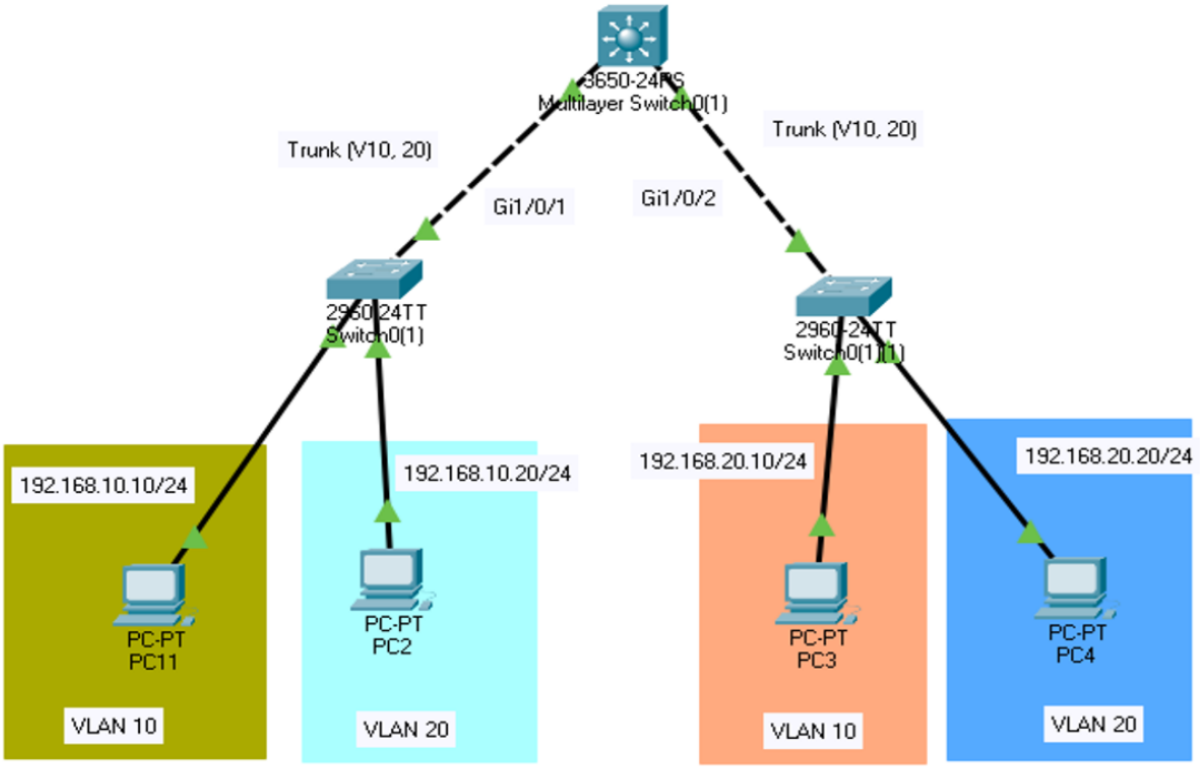

Figure .5: Layer 3 switch inter-VLAN routing with trunk

Table .4: Addressing table for topology 3

PC	Switch	VLAN	IP	Gateway
PC1	L2-A	VLAN 10	192.168.10.10	192.168.10.1
PC1	L2-A	VLAN 20	192.168.20.10	192.168.20.1
PC1	L2-B	VLAN 10	192.168.10.20	192.168.10.1
PC1	L2-B	VLAN 20	192.168.20.20	192.168.20.1

1. Configure this topology and test connectivity from all the devices. What do you notice, and what is the reason?

2. Why is a trunk port required between the Layer 3 switch and Layer 2 switches?

3. What is the function of a default gateway for each PC in this topology?

Conclusion

In this PW, the student learned how to configure inter-VLAN routing to enable communication between devices in different VLANs. Both the *router-on-a-stick* method and the use of a multi-layer (Layer 3) switch were explored, highlighting their respective advantages and limitations.

The exercises demonstrated how VLANs can segment a network into logical groups, improving security, traffic management, and overall organization. By configuring switched virtual interfaces (SVIs) and enabling routing on a Layer 3 switch, devices in separate VLANs were able to communicate efficiently without the need for an external router.

Through these configurations, the student developed a deeper understanding of the concepts of VLANs, inter-VLAN routing, trunk links, and the role of default gateways. Practical testing of connectivity reinforced the importance of proper IP addressing, VLAN assignments, and routing configurations.

This PW emphasized the benefits of using Layer 3 switches in modern networks, including reduced latency, improved performance, and simplified network design, while also providing hands-on experience with essential Cisco configuration commands and verification procedures.

PW 4: Creation of a network with redundant links. Simulation using Packet Tracer or practical work on real platforms.

I Learning objectives

By the end of this practical work, the student will be able to:

- Create a network topology with redundant links between switches.
- Identify the potential problems caused by redundant connections, such as Layer 2 loops and broadcast storms.
- Describe the role and functioning of the STP in preventing loops in a switched network.
- Configure STP on Cisco switches using Packet Tracer and observe how it manages redundant links.
- Analyze the STP topology using commands like `show spanning-tree` to identify the root bridge and blocked ports.
- Demonstrate how STP recalculates the topology and activates backup links when a primary link fails.
- Evaluate the impact of STP on network stability, efficiency, and fault tolerance in Layer 2 environments.
- Observe how the network automatically switches to a backup link when the main link fails.

II Theoretical background

II.1 Redundant links

Network redundancy refers to the inclusion of additional switches, links, and communication paths within a network to improve its reliability and ensure continuous data transmission. The

main purpose is to keep the network operational even if one component, cable, or switch fails [8].

II.2 Importance of redundancy

In a well-structured Layer 2 network, redundancy is a key design element. By including multiple switches and backup physical links, the network can continue to function even if one connection or device fails. This eliminates single points of failure and ensures uninterrupted service for users [8].

II.3 Problems caused by redundancy

Adding redundant connections can also lead to Layer 2 loops. A loop occurs when there are multiple active paths between switches, allowing Ethernet frames to circulate endlessly through the network. This creates excessive traffic, known as a **broadcast storm**, which can disrupt communication completely [9].

This situation is similar to an audio feedback loop at a concert: when the microphone picks up sound from the loudspeaker and re-amplifies it repeatedly, producing a loud, continuous noise. In networking, a similar feedback of data frames can make the network unusable.

To prevent such problems, the spanning tree protocol (STP) was developed. STP automatically detects redundant paths and places one or more of them in a blocking state to maintain a loop-free topology. If a failure occurs in the active path, STP quickly recalculates the network topology and reactivates the previously blocked link to restore connectivity [9].

Figure .1 illustrates the normal operation of STP, where all switches participate in the protocol, and one path is selected as the active forwarding route while redundant links remain in standby. Figure .2 shows how STP responds to a failure, dynamically re-evaluating the network and activating the backup link to ensure that communication between switches continues without interruption.

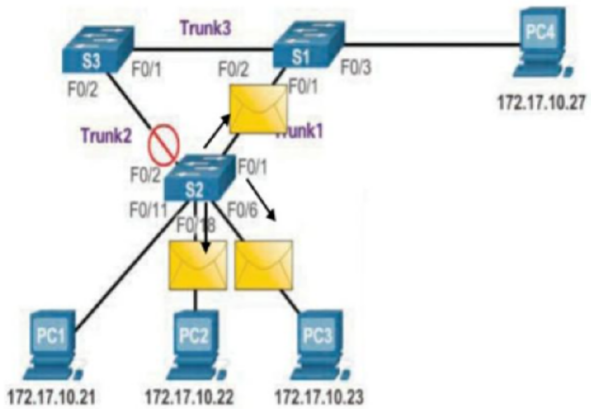

Figure .1: Normal operation of STP [7]

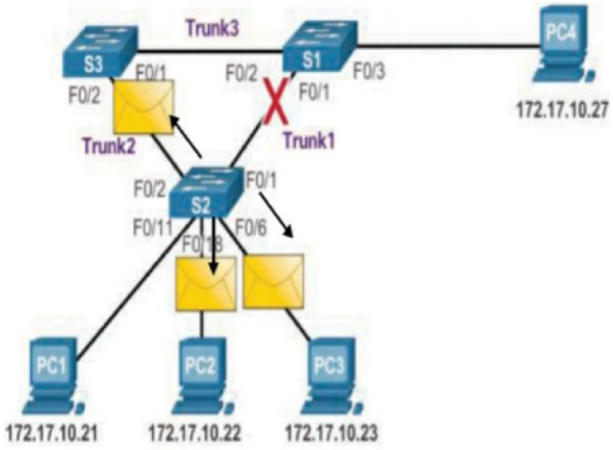

Figure .2: STP responds to a failure [7]

III Spanning tree protocol (STP)

III.1 Purpose of STP

The STP was created to prevent Layer 2 loops in redundant network topologies. It ensures there is always one active path between any two devices while keeping alternative paths available for failover [8].

III.2 How STP works

STP builds a logical loop-free tree structure by selecting one switch as the root bridge (RB) and calculating the shortest path from all other switches to it. Any redundant links that could create loops are placed in a blocking state, while only the optimal path remains active. If a failure occurs, STP recalculates the network and activates the backup link automatically [8].

III.3 The STP port states

Each port in STP can operate in several states [10]:

- **Blocking**: Prevents data forwarding to avoid loops.
- **Listening**: Participates in STP calculations.
- **Learning**: Learns MAC addresses but does not forward traffic.
- **Forwarding**: Actively forwards frames.
- **Disabled**: Administratively turned off.

III.4 Example of operation

During normal conditions, STP maintains a single active path between switches. When a link fails, it immediately brings a previously blocked port into service to restore communication. This process ensures both network stability and high availability [10].

IV Types of STP

Different versions of STP have been developed to improve efficiency and convergence time [10]:

- **STP (IEEE 802.1D)**: The original version, stable but slow (30–50 seconds).
- **RSTP (IEEE 802.1w)**: Rapid STP, providing faster recovery (under 10 seconds).
- **MSTP (IEEE 802.1s)**: Multiple STP, allowing several VLANs to share one STP instance, improving scalability.

V STP timers

STP timers are time intervals used to control [10]:

- How often switches send bridge protocol data unit (BPDU) messages.
- How long ports stay in specific STP states.
- How quickly the network reacts to topology changes.

When a topology change occurs (e.g., a link failure):

1. The switch waits **Max Age** (20 sec) to confirm the root info is no longer valid.
2. The port moves to **Listening** state for 15 sec.
3. Then to **Learning** state for another 15 sec.
4. Finally, it enters **Forwarding** state.

The total convergence time = 20 + 15 + 15 = 50 seconds.

These timers basically determine how fast or slow STP stabilizes. The three main timers are summarized in Table .1.

Table .1: STP main timers

Timer	Default value	Description
Hello time	2 seconds	How often does the Root Bridge send BPDU (Bridge Protocol Data Unit) messages to other switches to maintain the STP topology
Forward delay	15 seconds	The amount of time a port spends in the Listening and Learning states before it moves to the Forwarding state.
Max age	20 seconds	The maximum time a switch keeps STP information (BPDU) before it is considered outdated and discarded.

VI STP path cost

In STP, each link is assigned a **path cost** that helps switches determine the best path to reach the Root Bridge. The total path cost is calculated as the sum of the costs of all links between a switch and the Root Bridge

A lower path cost indicates a faster and more preferred link. Therefore, high-speed links such as Gigabit Ethernet have lower costs compared to slower links like Fast Ethernet. STP always selects the path with the lowest cumulative cost to forward traffic. Table .2 shows the standard STP path cost values based on link speed [11].

Table .2: STP costs

Link type / speed	STP path cost (Old standard)	STP path cost (IEEE 802.1D-2004)
10 Mbps (Ethernet)	100	2,000,000
100 Mbps (Fast Ethernet)	19	200,000
1 Gbps (Gigabit Ethernet)	4	20,000
10 Gbps (10-Gigabit Ethernet)	2	2,000
100 Gbps	–	200
1 Tbps (1000 Gbps)	–	20

VII Practical part

VII.1 Training-related knowledge

Topology: In this training, a simple and clear configuration uses three switches and three PCs in a redundant triangle topology. Open Cisco Packet Tracer and place three switches and three PCs. Connect them as shown in Figure .3. In addition, the host IP addressing configuration is shown in Table .3. The connections are as follows:

- PC1 → SW1 (Fa0/1)
- PC2 → SW2 (Fa0/1)

- PC3 → SW3 (Fa0/1)
- SW1–SW2 (Fa0/2 ↔ Fa0/2)
- SW1–SW3 (Fa0/3 ↔ Fa0/3)
- SW2–SW3 (Fa0/4 ↔ Fa0/4)

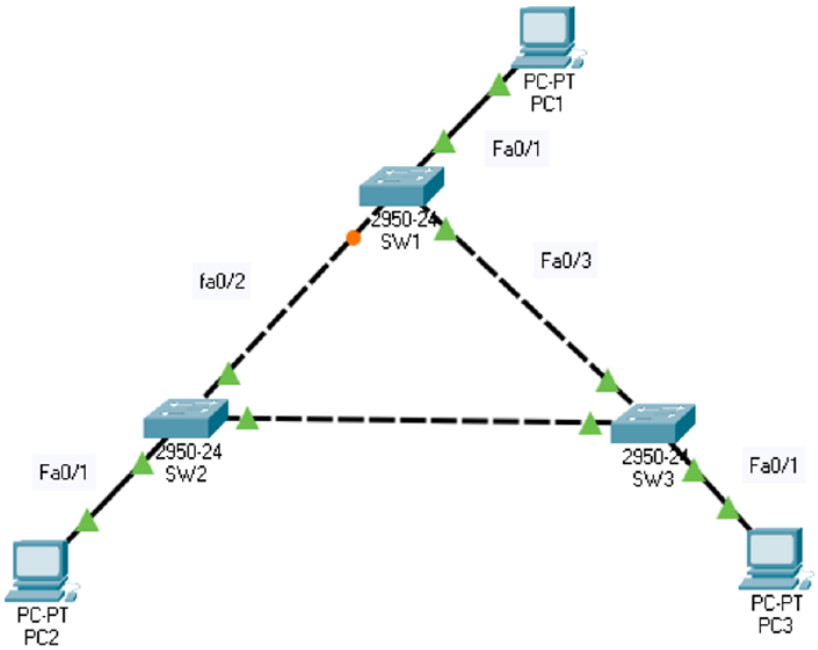

Figure .3: Network topology for STP

Table .3: Addressing configuration of host IPs

PC	IP Address	Subnet Mask	Default Gateway
PC1	192.168.1.1	255.255.255.0	192.168.1.254
PC2	192.168.1.2	255.255.255.0	192.168.1.254
PC3	192.168.1.3	255.255.255.0	192.168.1.254

1. First, enable STP on each switch (STP is enabled by default, but we configure specific parameters to observe its behavior). Before starting, change the hostnames of the switches to `SW1`, `SW2`, and `SW3`. The switch with the lowest priority will become the Root Bridge.

```
SW1(config)# spanning-tree mode pvst
SW1(config)# spanning-tree vlan 1 priority 24576
%Perform the same configuration on SW2 and SW3.
```

2. Now, verify the STP status on each switch by typing the following command:

```
SW1# show spanning-tree
```

3. Which switch is elected as the Root Bridge? Explain why.
4. Which ports are in the **Forwarding** state?
5. Which ports are in the **Blocking** state?
6. Why is the link between `SW1` and `SW2` shown in orange color?
7. Test network redundancy:
   - Disconnect the link between `SW1` and `SW3`.
   - Wait a few seconds.
   - Run the following command again on `SW2`:

```
SW2# show spanning-tree
```

8. Observe how STP recalculates the topology. Notice that the previously blocked port automatically transitions to the **Forwarding** state.
9. Replace one FastEthernet link (`Fa0/x`) with a GigabitEthernet link (`Gi0/1`).
10. Observe how the STP path cost changes. The faster GigabitEthernet link usually becomes the preferred path. Verify the result.
11. Change the STP mode to Rapid-PVST using the following command:

```
Switch(config)# spanning-tree mode rapid-pvst
```

12. Repeat the cable disconnection test. Observe how Rapid-PVST converges much faster (within 1–2 seconds).
13. What problem does STP solve in a network with redundant links?
14. What happens to the ports that are not used to reach the Root Bridge?
15. How long does STP take to reconverge after a link failure?
16. What difference do you observe when replacing a FastEthernet link with a GigabitEthernet link?
17. What would happen if STP were disabled in this topology?

Conclusion

In this PW, the student learned how to design and configure a network with redundant links while ensuring loop-free operation using the STP. The exercises demonstrated how redundant physical connections between switches improve network reliability and fault tolerance, allowing continuous communication even if a link fails.

Through hands-on configuration in Cisco Packet Tracer, the student observed how STP elects a Root Bridge, places redundant ports in a blocking state, and recalculates the network topology automatically when a link goes down. The impact of STP port states, path cost, and different STP modes such as PVST and Rapid-PVST was explored, showing how they affect convergence time and network efficiency.

Practical testing also highlighted the importance of proper link speed consideration, as faster links are preferred due to lower path costs. Overall, this work reinforced the significance of STP in maintaining network stability, preventing broadcast storms and loops, and ensuring that backup links are available for automatic failover in redundant network topologies.

PW 5: Configuration of the Ether Channel protocol between switches. Simulation using Packet Tracer or practical work on real platforms.

I Learning objectives

By the end of this practical work, the student will be able to:

- Understand the concept and purpose of EtherChannel.
- Configure EtherChannel using LACP (Link Aggregation Control Protocol, IEEE 802.3ad) and PAgP (Port Aggregation Protocol, Cisco proprietary).
- Verify the operation and status of EtherChannel.
- Troubleshoot common EtherChannel problems.

II Theoretical background

II.1 EtherChannel protocols

EtherChannel is a link aggregation technology that combines several physical Ethernet links into one logical interface called a Port-Channel (as shown in Figure .1). This logical interface increases bandwidth, provides redundancy, and improves network stability. If one physical link fails, traffic continues to flow through the remaining links, ensuring high availability.

In fact, EtherChannel also optimizes STP performance because STP treats the entire Port-Channel as a single link, avoiding unnecessary blocking of individual ports and improving convergence [12].

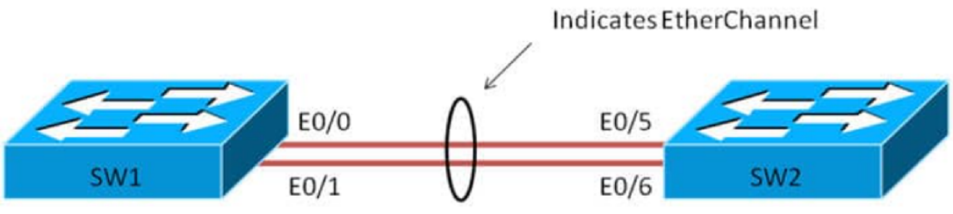

Figure .1: Sample EtherChannel physical layout [13]

There are three ways to form EtherChannel [12]:

1. **LACP (802.3ad)**: Standard protocol, widely used (Modes: active and passive).
2. **PAgP**: Cisco proprietary (Modes: desirable and auto).
3. **Manual (ON)**: Forces aggregation without negotiation (must match on both sides).

All physical ports in an EtherChannel must have identical settings (speed, duplex, trunk/access mode, allowed VLANs). Traffic load balancing is performed using algorithms based on MAC/IP addresses or port numbers. The EtherChannel improves bandwidth, reliability, and overall network efficiency, making it essential in modern switching environments [12].

II.2 EtherChannel and STP

STP sees the entire EtherChannel bundle as one logical link. This provides several benefits [12]:

- STP recalculations are faster
- No physical member port is blocked by STP
- Loop prevention is maintained
- Redundancy is preserved within the EtherChannel itself

II.3 Load balancing methods

Switches distribute traffic across links based on hashing algorithms that use fields such as follows [12]:

- Source MAC
- Destination MAC
- Source IP
- Destination IP
- TCP/UDP ports

Cisco uses XOR-based hashing to decide which physical port carries each frame. Each switch chooses its own load-balancing method; it does not need to match the other switch [12].

II.4 Advantages and disadvantages of EtherChannel

The EtherChannel increases bandwidth by combining several physical links into one logical connection, providing higher throughput, redundancy, and better STP performance. It also simplifies management and supports load balancing across the bundled interfaces [14].

However, it has some limitations: all ports must be configured identically, troubleshooting can be more complex, traffic may not always be evenly balanced, and the number of supported links is limited. Despite these drawbacks, EtherChannel remains an effective way to improve link capacity and reliability in switched networks [14].

III Practical part

III.1 Training-related knowledge for topology 1

Topology 1: This topology consists of two switches, SW1 and SW2, connected using two FastEthernet links (Fa0/1 and Fa0/2) as shown in Figure .2. The main aim is to configure these links as an EtherChannel using the LACP (802.3ad) negotiation protocol defined in IEEE 802.3ad. In this setup, SW1 operates in **active mode**, initiating the negotiation, while SW2 is configured in **passive mode**, responding to LACP packets. Together, these interfaces will form a single logical Port-Channel that provides increased bandwidth, redundancy, and improved link management.

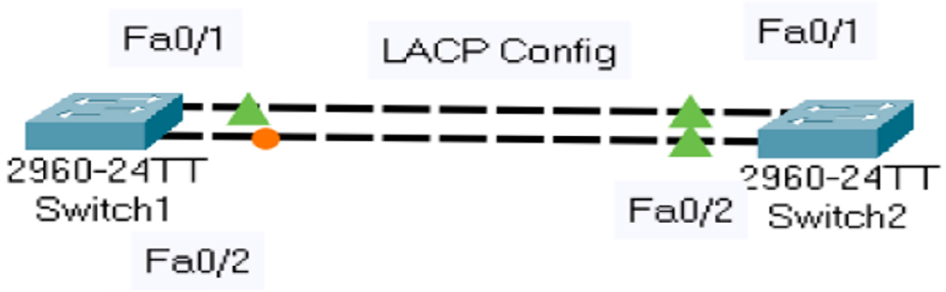

Figure .2: Network topology 1 for EtherChannel LACP configuration

1. First step is to configure the basic switch.
2. Configure trunk mode on the user interfaces.
3. Create EtherChannel using LACP: SW1 as active, SW2 as passive:

```
S1> enable
S1# configure terminal
S1(config)# hostname S1
S1(config)# interface range fa0/1 - 2
```

```
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk allowed vlan all
S1(config-if-range)# channel-group 1 mode active
S1(config-if-range)# exit
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan all
S1(config-if)# exit
% Same steps for Switch 2
```

4. Now, verify EtherChannel operation for both switches. Use the following commands:

```
S1# show etherchannel summary
S2# show interfaces port-channel 1
S1# show spanning-tree
```

Questions

1. What is the role of the active and passive modes in LACP?
2. What will happen if both switches are configured as passive?
3. Why must all physical ports have identical configurations before forming an EtherChannel?
4. How does STP see the Port-Channel interface?

III.2 Training-related knowledge for topology 2

Topology 2: This topology features two switches, SW2 and SW3, connected through two physical links on interfaces Fa0/3 and Fa0/4 (Figure .3). Students will configure these links to form an EtherChannel using the Cisco proprietary protocol PAgP. In this configuration, SW2 operates in desirable mode, actively initiating aggregation, while SW3 is set to auto, waiting for negotiation. Once successfully formed, the Port-Channel will combine both links into a single logical connection that enhances throughput and resiliency.

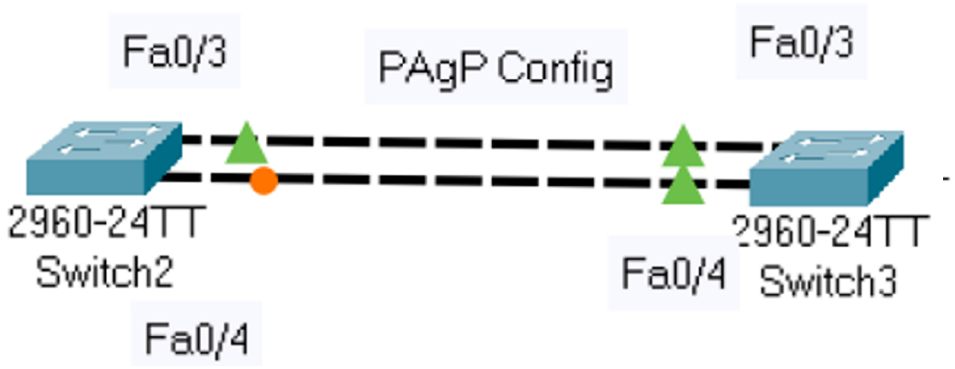

Figure .3: Network topology 2 for EtherChannel PAgP configuration

1. First step is to configure trunk mode on interfaces using the following commands:

```
S2(config)# interface range fa0/3 - 4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk allowed vlan all
S2(config-if-range)# channel-group 2 mode desirable
S2(config-if-range)# exit
S2(config)# interface port-channel 2
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk allowed vlan all
S2(config-if)# exit
% Same steps for Switch 3
```

2. Create EtherChannel using PAgP.

3. Now, verify EtherChannel formation for both switches. Use the following commands:

```
S2# show etherchannel summary
S3# show pagp neighbor
S3# show interfaces port-channel 2
```

4. Compare PAgP with LACP.

Questions

1. What is the difference between **desirable** and **auto** modes?

2. Will PAgP EtherChannel form if both switches are set to **auto**? Why?

3. Why is PAgP not recommended for multi-vendor environments?

4. What is the difference between LACP and PAgP in terms of standardization?

III.3 Training-related knowledge for topology 3

Topology 3: This topology includes two switches, SW1 and SW3, interconnected using two FastEthernet links on ports Fa0/5 and Fa0/6 (Figure .4). Unlike the previous topologies, EtherChannel will be configured manually using mode ON, which forces link aggregation without using any negotiation protocol. Both switches must be configured identically for the PortChannel to form correctly. This topology highlights the simplicity of manual EtherChannel while demonstrating the potential risks of misconfiguration due to the lack of protocol verification.

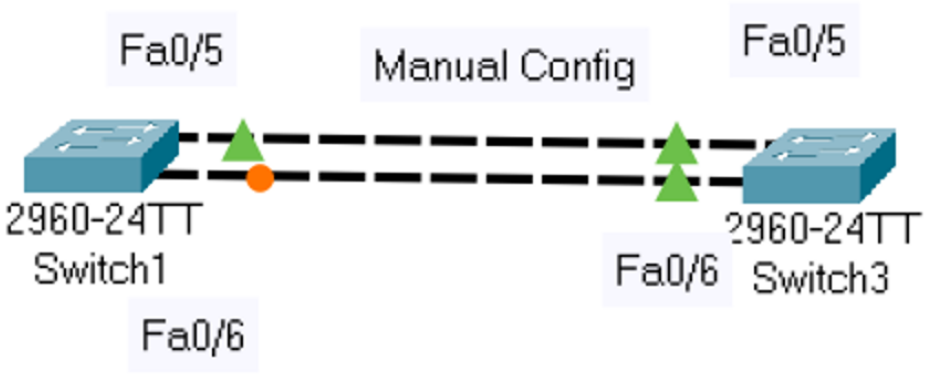

Figure .4: Network topology 3 for EtherChannel manual configuration

1. First step is to configure the trunk on all ports using the following commands:

```
S1(config)# interface range fa0/5 - 6
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk allowed vlan all
S1(config-if-range)# channel-group 3 mode on
S1(config-if-range)# exit
S1(config)# interface port-channel 3
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan all
S1(config-if)# exit
% Same steps for Switch 3
```

2. Force EtherChannel without negotiation using mode ON.

3. Observe the risks related to this mode.

4. Verify link aggregation using the following commands:

```
S1# show etherchannel summary
S3# show interfaces port-channel 3
```

Questions

1. Why is mode ON considered risky compared to LACP and PAgP?
2. What happens if one switch is set to ON and the other is not?
3. Why is manual EtherChannel not recommended in large networks?
4. Which EtherChannel mode provides the best protection against misconfiguration?

Conclusion

In this PW, the student explored the configuration and operation of EtherChannel as a method for aggregating multiple physical links into a single logical connection between switches. The experiments demonstrated how EtherChannel increases available bandwidth, improves redundancy, and enhances overall network stability while simplifying link management.

Through hands-on configurations, EtherChannel was implemented using LACP, PAgP, and manual (ON) modes. The use of LACP highlighted the advantages of a standardized and negotiation-based protocol, offering better protection against misconfiguration, especially in multi-vendor environments. PAgP illustrated Cisco's proprietary approach, while the manual mode emphasized the risks associated with forced aggregation without protocol verification.

The interaction between EtherChannel and STP was also observed, showing that STP treats the Port-Channel as a single logical link, which prevents unnecessary port blocking and improves convergence behavior. Verification commands allowed the student to confirm correct bundle formation, load balancing, and operational status of the Port-Channel interfaces.

This PW reinforced the importance of EtherChannel in modern switched networks, providing an efficient solution for bandwidth aggregation, fault tolerance, and optimized Layer 2 topology design.

PW 6: Implementation of static routing. Simulation using Packet Tracer or practical work on real platforms.

I Learning objectives

In this practical work, the student will:

- Understand the concept of routing and its importance in interconnecting multiple networks.
- Explore the principles of static routing, including route definition, next-hop identification, and routing table behavior.
- Configure static routes on Cisco routers using Cisco Packet Tracer to establish communication between different networks.
- Verify and test connectivity using commands such as `ping`, `traceroute`, and `show ip route`.
- Analyze the advantages and limitations of static routing in comparison with dynamic routing.
- Develop troubleshooting skills by identifying and correcting common static routing configuration errors.

II Theoretical background

II.1 Static routing

Routing is a fundamental concept in computer networking as it determines how data packets are directed within a network. Routing is essential because it allows computers to communicate with other devices, even when they are not part of the same network or subnet. The routing process involves making decisions about the best path for packets to reach their intended destinations [5].

Static routing is a fundamental concept in computer networking that involves manually configuring routing tables on network devices to determine the path data should take within a

network. In this practical exercise, we will use Cisco Packet Tracer, a network simulation tool, to learn and practice the basics of static routing [5].

II.2 Principles of static routing

In static routing, each router must have a predefined path to reach every possible destination network. The route entries are stored in the router's routing table and specify the destination network, subnet mask, and next-hop address or outgoing interface. If the network topology changes, the administrator must manually update the route entries. For this reason, static routing is ideal for networks with stable topologies [8].

II.3 Metric in static routing

In static routing, the metric is used to determine the priority of routes when there are multiple static routes to the same network. When a static route is created, the router stores it in the routing table with a default metric value of 1, as the router considers the route direct and preferred [8, 15].

The network administrator can manually change the metric to prioritize one route over another or to make a route act as a backup. A route with a lower metric is preferred and used first, while a route with a higher metric is only used if the primary route becomes unavailable (Figure .1).

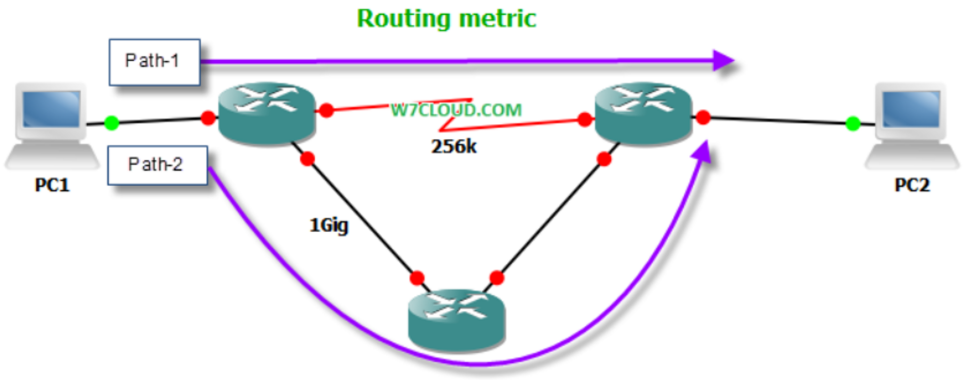

Figure .1: Choosing the best routing path using metric [15]

Unlike dynamic routing, static routes do not calculate the metric automatically; it depends entirely on the value assigned by the administrator. For example, if a router has two static routes to the same network, one with a metric of 1 and the other with a metric of 5, the router will automatically choose the route with the lower metric and use the other as a backup. This allows the metric in static routing to provide precise control over route priorities between different networks.

II.4 Advantages and disadvantages

Advantages [16]:

- Simple to configure and manage on small networks.
- No bandwidth consumption for routing updates.
- High control and predictable routing behavior.

Disadvantages [16]:

- Not scalable for large or dynamic networks.
- Manual updates required when topology changes.
- Human error risk during configuration.

III Practical part

III.1 Training-related knowledge for topology 1

Topology 1: In this topology (Figure .2), the network consists of one router, two switches, and two PCs. Each PC is connected to the router through its respective switch, forming two separate local area networks (LANs). The goal of this configuration is to establish communication between the two PCs by configuring basic routing on the router. The IP addressing scheme used for this topology is presented in Table .1.

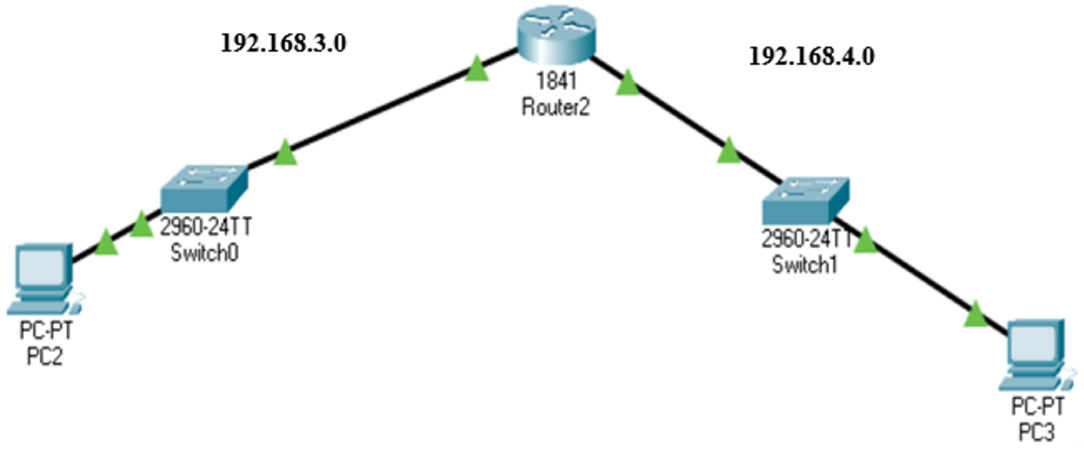

Figure .2: Network topology 1 for basic router configuration

Table .1: Router interfaces and network addressing for basic router configuration

Network	Router Interface	IP Address	Subnet Mask
Network 1 (192.168.3.0/24)	G0/0	192.168.3.1	255.255.255.0
Network 2 (192.168.4.0/24)	G0/1	192.168.4.1	255.255.255.0

1. First step is to configure IP addresses on the interfaces for the router and PCs using the following commands:

```
Router1> enable
Router1# configure terminal
Router1(config)# interface GigabitEthernet0/0
Router1(config-if)# ip address XXX.XXX.X.X 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# exit
%Same steps are applied for the interface G0/1.
```

2. After assigning IP addresses to PC1 and PC2, what happens when you try to ping from PC1 to PC2?

III.2 Training-related knowledge for topology 2

Topology 2: In this topology (Figure .3), the network consists of two routers, two switches, a serial cable, and two PCs. Each PC is connected to its respective router through a switch, forming two separate LANs. The routers are interconnected via a serial link to enable communication between the two LANs. The goal of this configuration is to establish communication between the two PCs by configuring static routing on both routers. The IP addressing scheme used for this topology is presented in Table .2.

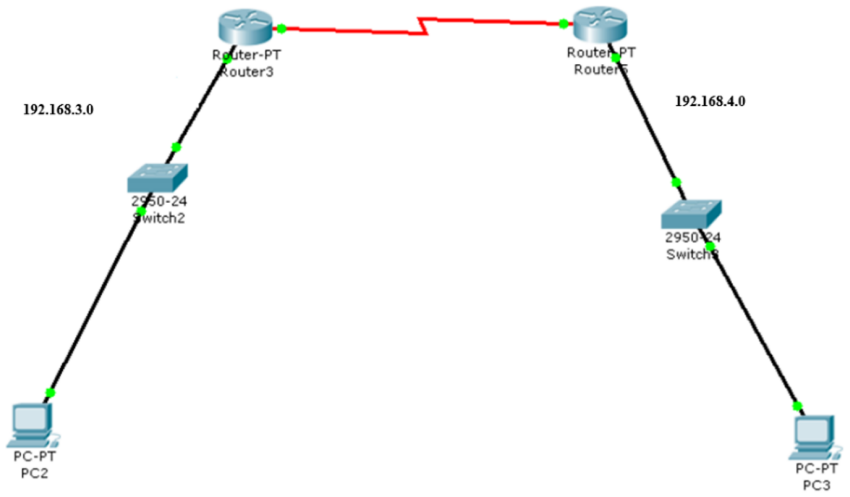

Figure .3: Network topology 2 for static routing with two routers

Table .2: Router interfaces and network addressing for static routing

Network	Router Interface	IP Address	Subnet Mask
LAN 1 (192.168.3.0/24)	R1 G0/0	192.168.3.1	255.255.255.0
LAN 2 (192.168.4.0/24)	R2 G0/0	192.168.4.1	255.255.255.0
Serial Link (10.0.0.0/30)	R1 S0/0/0	10.0.0.1	255.255.255.252
Serial Link (10.0.0.0/30)	R2 S0/0/0	10.0.0.2	255.255.255.252

1. Now, assign IP addresses and test the connection between PC1 and PC2. What happens when you try to ping from PC1 to PC2?
2. Why does the ping fail? Explain in terms of network addressing and routing.
3. How would you solve the problem so that the PCs can communicate?
4. Now, let's configure static routing using the `ip route` command. Access the router CLI and enter configuration mode:

```
R1> enable
R1# configure terminal
R1(config)# interface serial0/0/0
% Set the clock rate (for example, 64000 bps)
R1(config-if)# clock rate 64000
R1(config)# ip route 192.168.4.0 255.255.255.0 10.0.0.2
R1(config)# exit
% Same steps for the interface G0/1
```

5. Now, try the connection again between PC1 and PC2. What are the results?
6. Why is a serial link needed between the two routers?
7. What is the role of the static route on each router?
8. What happens if you forget to configure the static route on R2?
9. How would you extend this network to add another LAN behind R1?
10. Compare this two-router topology with the single-router topology in terms of routing complexity.

III.3 Training-related knowledge for topology 3

Topology 3: In this topology (Figure .4), the network consists of four routers, four switches, and four PCs, with the routers connected in a circular (ring) topology. Each PC is connected to

its respective router through a switch, forming four separate LANs. The routers are interconnected via Ethernet links to enable communication across the entire network. The goal of this configuration is to establish end-to-end communication between all PCs by configuring static routing on each router. The IP addressing scheme used for this topology is presented in Table .3.

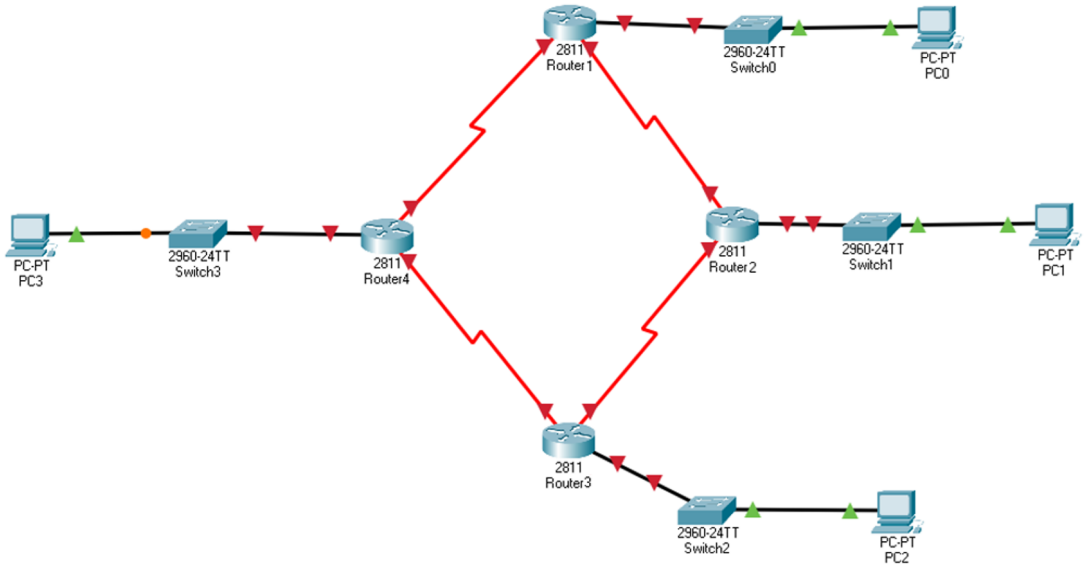

Figure .4: Network topology 3 for static routing ring with PCs

Table .3: IP Addressing table of topology 3 for static routing

Device	**Interface**	**IP Address**	**Subnet Mask**	**Connected To**
R1	F0/0	10.0.12.1	255.255.255.0	R2
R1	F0/1	10.0.14.1	255.255.255.0	R4
R1	F0/2	192.168.1.1	255.255.255.0	PC1
R2	F0/0	10.0.12.2	255.255.255.0	R1
R2	F0/1	10.0.23.2	255.255.255.0	R3
R2	F0/2	192.168.2.1	255.255.255.0	PC2
R3	F0/0	10.0.23.3	255.255.255.0	R2
R3	F0/1	10.0.34.3	255.255.255.0	R4
R3	F0/2	192.168.3.1	255.255.255.0	PC3
R4	F0/0	10.0.34.4	255.255.255.0	R3
R4	F0/1	10.0.14.4	255.255.255.0	R1
R4	F0/2	192.168.4.1	255.255.255.0	PC4
PC1	NIC	192.168.1.2	255.255.255.0	R1 F0/2
PC2	NIC	192.168.2.2	255.255.255.0	R2 F0/2
PC3	NIC	192.168.3.2	255.255.255.0	R3 F0/2
PC4	NIC	192.168.4.2	255.255.255.0	R4 F0/2

1. Now, make the static routing for all routers. For example, for Router 1, follow these commands:

```
R1> enable
R1# configure terminal
R1(config)# interface f0/0
R1(config-if)# ip address 10.0.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface f0/1
R1(config-if)# ip address 10.0.14.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface f0/2
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ip route 10.0.23.0 255.255.255.0 10.0.12.2
R1(config)# ip route 10.0.34.0 255.255.255.0 10.0.14.4
R1(config)# ip route 192.168.2.0 255.255.255.0 10.0.12.2
R1(config)# ip route 192.168.3.0 255.255.255.0 10.0.14.4
R1(config)# ip route 192.168.4.0 255.255.255.0 10.0.14.4
R1(config)# end
R1# write
```

   Same steps are applied for all other routers.

2. Now, after configuring static routing, test the connectivity for all the PCs.

3. Turn off or remove Router R2 from the topology. What happens to the communication between all PCs after R2 is removed?

4. Which PCs can still communicate successfully, and through which path?

5. Which PC(s) lose connectivity entirely, and why?

6. Explain why some connections still work even after R2 is removed, while others fail.

Conclusion

In this PW, the student studied the principles and implementation of static routing as a fundamental method for enabling communication between multiple networks. Through a series of progressively complex topologies, the role of routers in forwarding packets between different LANs was clearly demonstrated.

By configuring static routes manually, the student observed how routing tables determine packet paths using destination networks, subnet masks, next-hop addresses, and metrics. Connectivity tests using commands such as `ping`, `traceroute`, and `show ip route` confirmed the correct operation of static routing and helped identify common configuration errors.

The experiments also highlighted the strengths of static routing, including simplicity, predictability, and low overhead, as well as its limitations in terms of scalability and adaptability to topology changes. Failure scenarios showed that static routes do not automatically recover from link or router outages, emphasizing the need for careful planning or backup routes.

This PW reinforced the importance of static routing in small and stable network environments and provided a solid foundation for understanding more advanced routing concepts, including dynamic routing protocols and fault-tolerant network design.

PW7: Implementation of dynamic routing (RIPv2, EIGRP, and OSPF). Simulation using Packet Tracer or practical work on real platforms.

I Learning objective

In this practical work, the student will:

- Understand the fundamental concepts of dynamic routing and how it differs from static routing.
- Configure and verify RIPv2, EIGRP, and OSPF routing protocols on Cisco routers.
- Analyze the behavior of each dynamic routing protocol in terms of convergence, scalability, and efficiency.
- Observe how routers automatically update routing tables in response to topology changes or link failures.
- Compare the advantages and limitations of RIPv2, EIGRP, and OSPF in different network environments.
- Test communication between end devices and interpret routing information using commands such as `show ip route`, `show ip protocols`, and protocol-specific debug commands.
- Develop troubleshooting skills by identifying and resolving routing configuration errors.
- Understand the concept of routing metrics, administrative distance, and path selection for each protocol.

II Theoretical background

II.1 Dynamic routing

Dynamic routing allows routers to automatically discover network paths and update their routing tables in response to changes in the network, such as link failures or congestion. For ex-

ample, when sending data from R1 (source) to R10 (destination), the normal path might be R1 → R2 → R5 → R9 → R10, which is chosen based on the routing metrics of the configured protocol. However, if R9 fails or becomes unreachable, the routers dynamically recalculate the route and redirect traffic through an alternative path, R1 → R2 → R5 → R8 → R10 (Figure .1), without manual intervention. This behavior demonstrates the key advantage of dynamic routing: automatic adaptation and fault tolerance, ensuring continued connectivity. Different protocols handle this rerouting differently: RIPv2 updates routes periodically and may converge more slowly, EIGRP recalculates affected routes quickly using its composite metrics, and OSPF floods link-state updates immediately to determine the new shortest path efficiently [17].

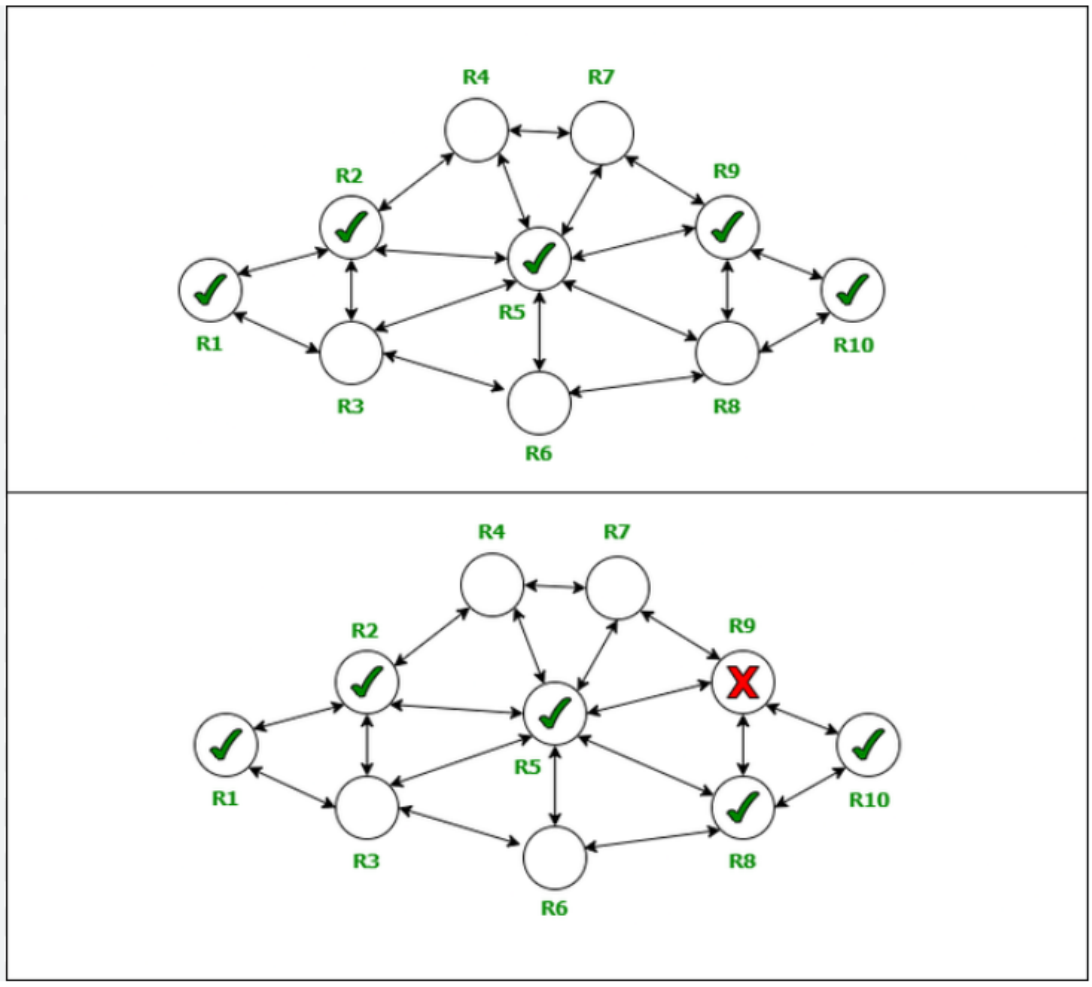

Figure .1: Dynamic routing [18]

Routing information protocol version 2 (RIPv2)

The RIPv2 is a distance-vector routing protocol that uses hop count as its metric to determine the best path to a destination. It supports classless routing classless inter-domain routing (CIDR), multicasting for route updates, and authentication. RIPv2 is simple to configure and suitable for small to medium networks, but it has limitations such as a maximum hop count of 15 and slower convergence compared to more advanced protocols. In this lab, RIPv2 allows students

to observe how routers exchange periodic updates and recalculate routes when a link fails [19].

Enhanced interior gateway routing protocol (EIGRP)

The EIGRP is a dynamic routing protocol that combines features of distance-vector and link-state protocols, often called a hybrid protocol. It calculates the best path using multiple metrics, including bandwidth, delay, load, and reliability, which allows for more efficient and flexible routing decisions than simple hop count. EIGRP adapts quickly to network changes, propagates updates only to routers affected by a topology change, and supports load balancing across multiple paths. Its rapid convergence and efficiency make it suitable for medium to large networks where fast adaptation is important [20]. The EIGRP properties are summarized as follow:
a. Number of jumps: 224 Next hop counts.
b. It divides the router into several zones called autonomous system AS.
c. Supports Summarization, variable length subnet mask (VLSM) and classless.

Open shortest path first (OSPF)

The OSPF is a widely used link-state routing protocol that maintains a complete map of the network topology. The OSPF is a widely used interior gateway protocol (IGP) in computer networking. It is designed to efficiently exchange routing information within an autonomous system (AS) (Figure .2) and calculate the shortest path to reach destination networks using Dijkstra's algorithm, based on link costs. OSPF is a link-state routing protocol, meaning that routers share detailed information about the state of their links with neighboring routers [21].

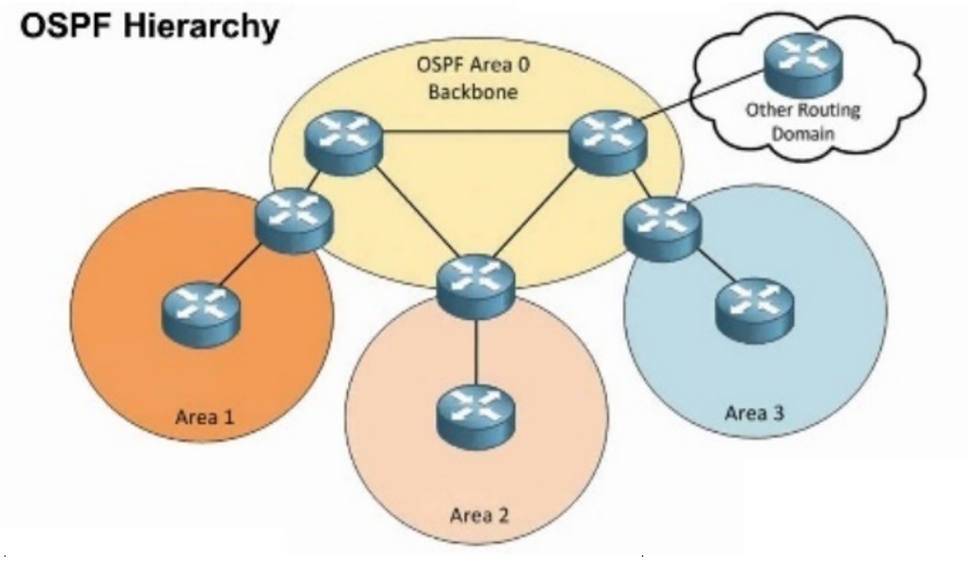

Figure .2: The OSPF protocol links autonomous systems [18]

III Practical part

III.1 Training-related knowledge for topology 1

Topology 1: In this topology, the network consists of three routers, four switches, and four PCs. Each PC is connected to the router through its respective switch, forming seven separate LANs. The goal of this configuration is to establish communication between the PCs by configuring the dynamic routing RIPv2 configuration on the routers. The IP addressing scheme used for this topology is presented Figure .3.

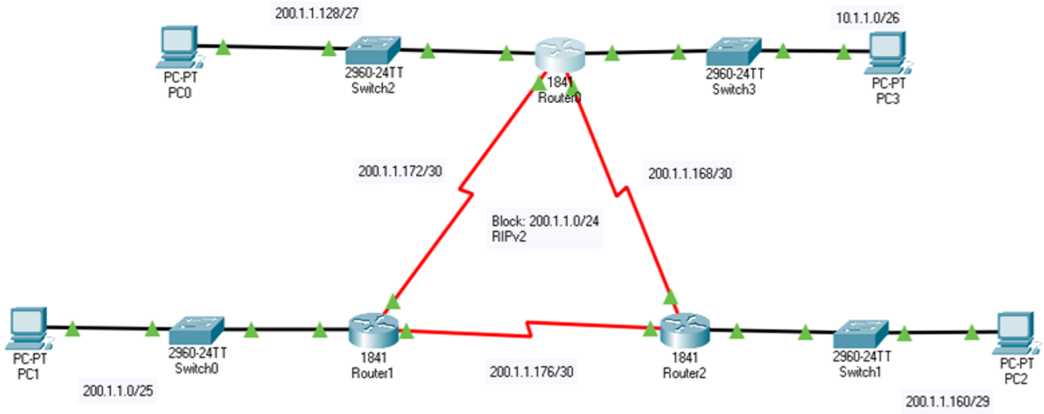

Figure .3: Network topology 1 for dynamic routing RIPv2

1. Make the configuration and change the hostnames of all routers to `R0`, `R1`, `R2`, and `R3`.

2. Configure IP addresses on the interfaces using the instructions below:

```
Router0> enable
Router0# configure terminal
Router0(config)# interface Fa0/0
Router0(config-if)# ip address 192.168.1.128 xxx.xxx.xxx.xxx
Router0(config-if)# no shutdown
Router0(config-if)# exit

Router0> enable
Router0# configure terminal
Router0(config)# interface serial0/0/0
Router0(config-if)# ip address 192.168.1.128 xxx.xxx.xxx.xxx
Router0(config-if)# no shutdown
Router0(config-if)# exit
%The same configuration to all router interfaces.
```

3. Now configure the dynamic routing RIPv2 for all routers:

```
! ---- RIPv2 ----
Router0(config)# router rip
Router0(config-router)# version 2
Router0(config-router)# no auto-summary
Router0(config-router)# network 192.168.1.0
Router0(config-router)# network 10.0.12.0
Router0(config-router)# network 10.0.41.0
Router0(config-router)# exit
% Apply similar configuration for all routers.
```

4. Now, check the interconnection between PCs using the `PING` command. What do you notice?

III.2 Training-related knowledge for topology 2

Topology 2: In this topology (Figure .4), the network consists of three routers, two switches, two serial cables, and two PCs. Each PC is connected to its respective router through a switch, forming four separate local area networks (LANs). The routers are interconnected via a serial link to enable communication between the two LANs. The goal of this configuration is to establish communication between the two PCs by configuring EIGRP dynamic routing the routers. The IP addressing scheme used for this topology is presented in Table .1.

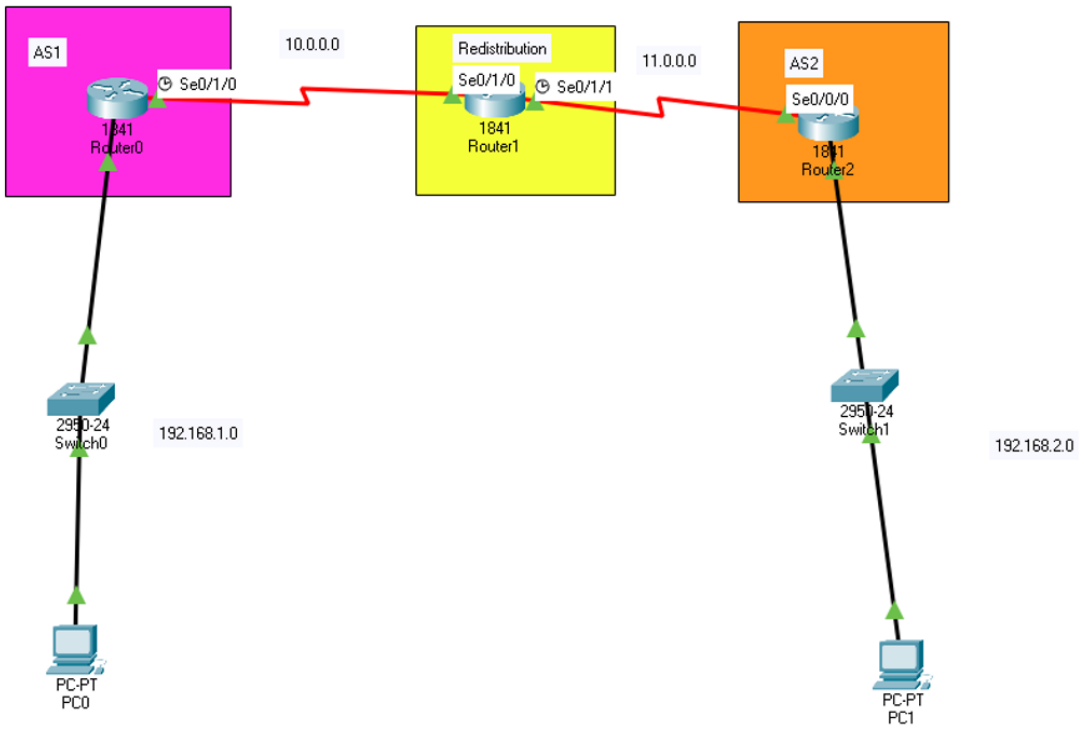

Figure .4: Network topology 2 for dynamic routing EIGRP

Table .1: Router interfaces and network addressing for EIGRP routing

Network	Router Interface	IP Address	Subnet Mask
LAN 1 (192.168.1.0/24)	R0 G0/0	192.168.1.1	255.255.255.0
LAN 2 (192.168.2.0/24)	R2 G0/0	192.168.2.1	255.255.255.0
Serial Link (10.0.0.0/30)	R0 S0/0/0	10.0.0.1	255.255.255.**xxx**
Serial Link (10.0.0.0/30)	R2 S0/0/0	10.0.0.2	255.255.255.**xxx**

1. Make the configuration. Use the router `EIGRP` command in global configuration mode to enable EIGRP on the router. Assign process ID `1` to the standalone system parameter. Use the wildcard option with the `network` command to advertise only the subnet and not the entire network by class.

   Note: A wildcard mask is the inverse of a subnet mask. Example: The inverse of subnet mask `255.255.255.252` is `0.0.0.3`. To compute the inverse, subtract the subnet mask from `255.255.255.255`:

   ```
     255.255.255.255
   - 255.255.255.252     Subtract subnet mask
   -------------------
     0.0.0.3
   ```

2. Enable the EIGRP routing protocol on all routers using the following commands:

   ```
   Router0> enable
   Router0# configure terminal
   Router0(config)# router eigrp 1
   Router0(config-router)# network 192.168.1.0 0.0.0.255
   Router0(config-router)# network 10.0.0.0 0.255.255.255
   Router0(config-router)# no auto-summary
   Router0(config-router)# exit
   Router0(config)# exit
   Router0# write memory

   % The same steps apply to Router2 (AS2).

   % Redistribution Router:
   Router0> enable
   Router0# configure terminal
   Router0(config)# router eigrp 1
   Router0(config-router)# network 10.0.0.0
   Router0(config-router)# no auto-summary
   ```

```
Router0(config-router)# redistribute eigrp 2
Router0(config-router)# exit

Router0(config)# router eigrp 2
Router0(config-router)# network 11.0.0.0
Router0(config-router)# no auto-summary
Router0(config-router)# redistribute eigrp 1
Router0(config-router)# exit
```

3. Now, check the interconnection between PCs using the `PING` command. What do you notice?

III.3 Training-related knowledge for topology 3

Topology 3: In this topology (Figure .5), the network consists of three routers, three switches, two serial cables, and three PCs. Each PC is connected to its respective router through a switch, forming four separate local area networks (LANs). The routers are interconnected via a serial link to enable communication between the two LANs. The goal of this configuration is to establish communication between the two PCs by configuring EIGRP dynamic routing on the routers. The IP addressing scheme used for this topology is presented in Table .2.

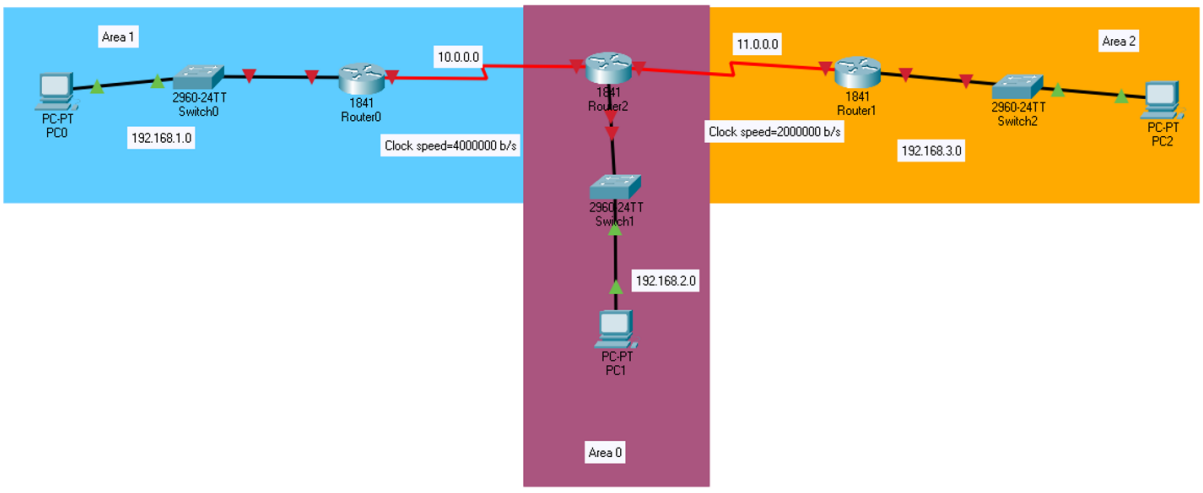

Figure .5: Network topology 3 for dynamic routing OSPF

Table .2: Router interfaces and network addressing for OSPF routing

Network	**Router Interface**	**IP Address**	**Subnet Mask**
LAN 1 (192.168.1.0/24)	R0 G0/0	192.168.1.1	255.255.255.0
LAN 2 (192.168.2.0/24)	R2 G0/0	192.168.2.1	255.255.255.0
Serial Link (10.0.0.0/30)	R0 S0/0/0	10.0.0.1 / 10.0.0.2	255.255.255.**xxx**
Serial Link (10.0.0.0/30)	R2 S0/0/0	11.0.0.1 / 11.0.0.2	255.255.255.**xxx**

1. First step is to configure IP addresses on the interfaces for the router and PCs using the following commands:

```
Router0> enable
Router0# configure terminal
Router0(config)# interface serial0/0/0
Router0(config-if)# ip address 10.0.0.0 255.0.0.0
Router0(config-if)# no shutdown
Router0(config-if)# exit
% The same conf for all the interfaces of the routers.
```

2. Now, configure the basic and simple OSPF routing configuration and enable OSPF on all routers (configure the clock speed on each serial interface).

3. Now, assuming that all routers are in a different OSPF area, each router will have information about the costs associated with the links. Calculate the total cost of the path.

4. On Router R2, use the command `show ip ospf neighbors`. Which routers are listed as neighbors?

5. What interface does R1 use to communicate with each neighbor?

   Router0 Configuration

```
Router0> enable
Router0# configure terminal
Router0(config)# router ospf 1
Router0(config-router)# network 192.168.1.0 x.x.x.x area 1
Router0(config-router)# network 10.0.0.0 x.x.x.x area 1
Router0(config-router)# exit
% The same manner conf for Router1.
```

   Router1 Configuration

```
Router1> enable
Router1# configure terminal
Router1(config)# router ospf 2
Router1(config-router)# network 192.168.2.0 x.x.x.x area 0
Router1(config-router)# network 10.0.0.0 x.x.x.x area 1
Router1(config-router)# network 11.0.0.0 x.x.x.x area 2
Router1(config-router)# exit
```

6. Now, check the interconnection between PCs using the PING command. What do you notice?

III.4 Training-related knowledge for topology 4

Topology 4: In this topology (Figure .6), the student will implement a large network OSPF routing configuration.

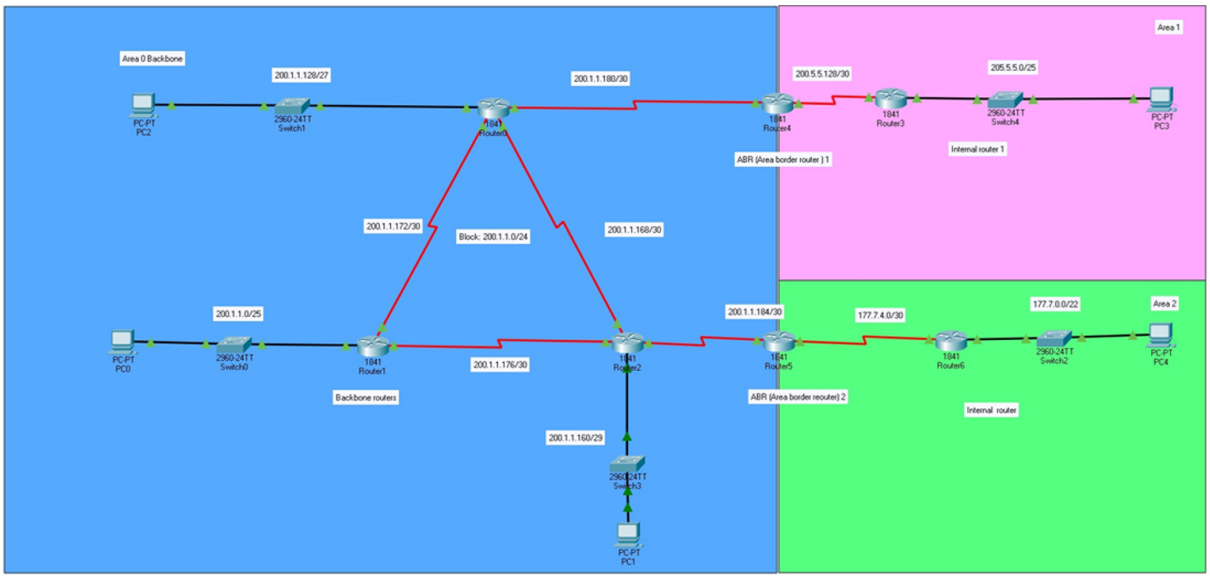

Figure .6: Network topology 3 for dynamic routing OSPF

1. Configure the basic and simple network OSPF in this topology.
2. Check the interconnection between PCs using the `PING` command.
3. Explain the purpose of the `clock rate` command in the serial interface configuration.
4. Why do we use EIGRP instead of RIPv2?
5. Explain the purpose of OSPF in dynamic routing.

Conclusion

In this PW, the student investigated the implementation and behavior of dynamic routing protocols, namely RIPv2, EIGRP, and OSPF, within different network topologies. The experiments demonstrated how dynamic routing enables routers to automatically discover network paths and update routing tables in response to topology changes or link failures.

By configuring RIPv2, the student observed the operation of a distance-vector protocol based on hop count metrics and periodic updates, highlighting its simplicity as well as its limitations in terms of convergence speed and scalability. The implementation of EIGRP illustrated faster convergence and more efficient routing decisions through the use of composite metrics and partial updates. OSPF configuration emphasized the advantages of a link-state protocol,

including accurate topology awareness, cost-based path selection, and scalability through area segmentation.

Connectivity tests and verification commands such as `ping`, `show ip route`, `show ip protocols`, and `show ip ospf neighbors` confirmed correct routing behavior and allowed the identification of protocol-specific characteristics. Failure and topology change scenarios further demonstrated the adaptability and fault tolerance of dynamic routing compared to static routing.

This PW reinforced the importance of dynamic routing protocols in modern networks, providing essential insight into protocol selection, network scalability, and efficient routing design for small, medium, and large-scale network environments.

General Conclusion

Throughout this practical workbook, we have explored both fundamental and advanced concepts of network configuration and routing on Cisco devices. Starting from the basic configuration of a switch (PW1), we progressively developed the skills required to manage VLANs and efficiently segment networks (PW2), before enabling communication between VLANs through inter-VLAN routing (PW3). The network reliability was then addressed by implementing redundant links (PW4) and enhancing bandwidth and fault tolerance using the EtherChannel protocol (PW5). Finally, both static routing (PW6) and dynamic routing protocols, including RIPv2, EIGRP, and OSPF (PW7), were configured and analyzed, allowing routers to automatically learn routes and manage network traffic efficiently.

These practical works followed a logical and incremental learning approach, where each experiment built upon the knowledge acquired in previous sessions. The students were exposed to real-world networking scenarios that involve scalability, convergence, redundancy, and protocol selection, which are essential aspects of modern network design. Through hands-on configuration and verification using Cisco IOS commands, the students improved their ability to interpret routing tables, diagnose connectivity issues, and understand the behavior of different routing mechanisms under normal and failure conditions.

By completing this workbook, students gained practical experience in configuring, testing, and troubleshooting network devices while reinforcing key theoretical concepts such as routing metrics, administrative distance, load balancing, and fault tolerance. The integration of multiple routing protocols and switching technologies provided a comprehensive view of how enterprise networks operate in practice.

Ultimately, this practical workbook offers a solid foundation for advanced networking studies and real-world network deployment. Equip students with the technical skills, analytical thinking, and confidence required to design, implement, and maintain reliable and scalable networks, while also serving as an effective preparation for professional networking careers and Cisco certification pathways.

List of Abbreviations

The following abbreviations and nomenclatures are used in this document:

BID	Bridge ID
LAN	Local area network
VLAN	Virtual local area network
PC	Personal computer
MAC	Media access control
TFTP	Trivial file transfer protocol
R&T	Networks and telecommunications
IP	Internet protocol
PING	Packet Internet or Inter-Network Groper
MHT	Microsoft HyperTerminal
VTY	Virtual teletype
IP	Internet protocole
TFTP	Trivial file transfer protocol
SNMP	Simple network management protocol
CLI	Command line interface
IOS	Internetwork operating system
NVRAM	Non-volatile random-access memory
SVIs	Switched virtual interfaces
STP	Spanning tree protocol
Rapid-PVST	Rapid per VLAN spanning tree
BPDU	Bridge Protocol Data Units
LACP	Link agregation control protocol
PAgP	Port agregation protocol
CIDR	Classless inter-domain routing
EIGRP	Enhanced interior gateway routing protocol
VLSM	Variable-length subnet masking
OSPF	Open shortest path first
RIPv2	Routing information protocol version 2

Bibliography

[1] A. S. Tanenbaum, "Network protocols," *ACM Computing Surveys (CSUR)*, vol. 13, no. 4, pp. 453–489, 1981.

[2] T. ANDREW S and W. DAVID J, *Computer networks*. Pearson, 2011.

[3] K. R. Kurose, "Computer networking: A top-down approach by james," *Kurose, Keith W. Ross*, p. 601, 2017.

[4] A. Cisco, "Cisco networking academy," *URL: https://www. netacad. com (in Eng)*, 2011.

[5] S. Keshav and S. Kesahv, *An engineering approach to computer networking: ATM networks, the Internet, and the telephone network*, vol. 116. Addison-Wesley Reading, 1997.

[6] A. Gupta, "How to configure vlan trunk." `https://www.learnabhi.com/how-to-configure-vlan-trunk/`, June 2018. Accessed: 24-Oct-2024.

[7] Cisco Networking Academy, "Switching, routing, and wireless essentials companion guide (ccnav7)." Archive.org link, 2021. Accessed: 24-Oct-2024.

[8] L. Toutain, *Réseaux locaux et Internet*. Hermes, 2003.

[9] F. Moskowitz, "The analysis of redundancy networks," *Transactions of the American institute of electrical engineers, part i: communication and electronics*, vol. 77, no. 5, pp. 627–632, 1958.

[10] S. Kasu, L. Hash, J. Marsh, R. Bull, *et al.*, *Spanning tree protocol*. PhD thesis, 2015.

[11] W. Huang, Y. Chen, and J. Hee, "Stp technology: An overview and a conceptual framework," *Information & management*, vol. 43, no. 3, pp. 263–270, 2006.

[12] Cisco, "Supports de cours cisco." `https://www.cisco.com/c/fr_ca/support/docs/lan-switching/etherchannel/98469-ios-etherchannel.html`, 2024. Accessed: 24-Nov-2024.

[13] S. Misra and S. Goswami, "Network routing: fundamentals, applications, and emerging technologies," 2017.

[14] Q. I. Ali and B. S. Mahmood, "Enhancement of industrial ethernet performance using modified etherchannel technique,"

[15] R. White, A. Retana, and D. Slice, *Optimal Routing Design*. Cisco Press, 2005.

[16] E. Akin and T. Korkmaz, "Comparison of routing algorithms with static and dynamic link cost in software defined networking (sdn)," *IEEE Access*, vol. 7, pp. 148629–148644, 2019.

[17] M. Murali Krishna, P. R. Mudimela, and P. P. Kumar, "Performance analysis of ripv2, ospf and eigrp protocols using cisco packet tracer simulator 7.2,"

[18] GeeksforGeeks, "Dynamic routing in computer networks." https://www.youtube.com/watch?v=RfwxV4VnOqI, 2024. Accessed: 09-Jan-2025.

[19] Cisco Community, "Ripv2 max hop count." https://community.cisco.com/t5/routing/ripv2-max-hop-count/m-p/2199055, 2021. Accessed: 09-Jan-2025.

[20] Cisco, "Cisco ios ip routing eigrp ipv6 configuration guide, 15-s." https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-s/ire-15-s-book/ip6-route-eigrp.pdf, 2015. Accessed: 01-Feb-2026.

[21] Cisco, "Cisco ios ip routing ospf configuration guide, xe-16." https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book.pdf, 2020. Accessed: 01-Feb-2026.